

# Nominal Unification from a Higher-Order Perspective

JORDI LEVY

Artificial Intelligence Research Institute (IIIA),  
Spanish Council for Scientific Research (CSIC)

and

MATEU VILLARET

Departament d'Informàtica i Matemàtica Aplicada (IMA),  
Universitat de Girona (UdG)

---

Nominal Logic is a version of first-order logic with equality, name-binding, renaming via name-swapping and freshness of names. Contrarily to higher-order logic, bindable names, called atoms, and instantiable variables are considered as distinct entities. Moreover, atoms are capturable by instantiations, breaking a fundamental principle of lambda-calculus. Despite these differences, nominal unification can be seen from a higher-order perspective. From this view, we show that nominal unification can be reduced to a particular fragment of higher-order unification problems: Higher-Order Pattern Unification. This reduction proves that nominal unification can be decided in quadratic deterministic time, using the linear algorithm for Higher-Order Pattern Unification. We also prove that the translation preserves most generality of unifiers.

Categories and Subject Descriptors: F.4.1 [Mathematical Logic and Formal Languages]:  
Mathematical Logic—*Lambda Calculus and Related Systems*

General Terms: Lambda Calculus, Nominal Logic, Automated Theorem Proving, Term Rewriting

Additional Key Words and Phrases: Higher-Order Pattern Unification, Nominal Unification

---

## 1. INTRODUCTION

*Nominal Logic* is a version of first-order many-sorted logic with equality and primitives for renaming via name-swapping, name-binding, and freshness of names. It is characterized by a syntactic distinction between *atoms* (that roughly correspond to the notion of bound variable) and *variables* (that would correspond to free variables). Therefore, binders can only bind atoms, we can only instantiate variables, and atoms are not instantiable even if they are not bounded. It also provides a *new-quantifier* [Gabbay and Pitts 1999], to model name generation and locality. Nominal logic was introduced at the beginning of this decade by Gabbay and Pitts [Gabbay and Pitts 1999; Pitts 2001; Gabbay and Pitts 2001; Pitts 2003].

---

This research has been partially funded by the CICYT research project TIN2007-68005-C04-01/02/03.

Permission to make digital/hard copy of all or part of this material without fee for personal or classroom use provided that the copies are not made or distributed for profit or commercial advantage, the ACM copyright/server notice, the title of the publication, and its date appear, and notice is given that copying is by permission of the ACM, Inc. To copy otherwise, to republish, to post on servers, or to redistribute to lists requires prior specific permission and/or a fee.

© 20YY ACM 1529-3785/20YY/0700-0001 \$5.00

These first works have inspired a sequel of papers where bindings and freshness are introduced in other areas, like nominal algebra [Gabbay and Mathijssen 2006; 2007; 2009], equational logic [Clouston and Pitts 2007], rewriting [Fernández and Gabbay 2005; 2007], unification [Urban et al. 2003; 2004], and Prolog [Cheney and Urban 2004; Urban and Cheney 2005].

This paper is concerned with *Nominal Unification*, the problem of deciding if two nominal terms can be made  $\alpha$ -equivalent by instantiating their variables by nominal terms. In this instantiation, variables are allowed to *capture* atoms. Urban, Pitts and Gabbay [Urban et al. 2003; 2004] describe a sound and complete, but inefficient (exponential), algorithm for nominal unification. Fernández and Gabbay [Fernández and Gabbay 2005] extend this algorithm to deal with the new quantifier and locality. Nominal Logic’s equivariance property suggested to Cheney [Cheney 2005a] a stronger form of unification called equivariant unification. He proves that equivariant unification and matching are NP-hard problems. Another variant of nominal unification is permissive unification, defined by Dowek, Gabbay and Mulligan [Dowek et al. 2009; 2010], that is also reducible to Higher-Order Pattern Unification. Calvès and Fernández describe in [Calvès and Fernández 2007] a direct but exponential implementation of a nominal unification algorithm in Maude, and in [Calvès and Fernández 2008] a polynomial implementation, based on the use of a graph representation of terms, and a lazy propagation of swappings. In [Levy and Villaret 2008] we prove that Nominal Unification can be decided in quadratic time by reduction to Higher-Order Pattern Unification. The present paper is an extension of this preliminary paper, where we have simplified the reduction by removing freshness equations, and we have included the proof of some important properties of pattern unifiers. In particular, we prove that most general higher-order pattern unifiers can be written without using other bound-variable names than the ones used in the presentation of the unification problem. Moreover, we establish a precise correspondence between most general nominal unifiers and most general pattern unifiers. Sections 4, 6 and 8 are completely new in this extended version. Recently, Calvès and Fernández [Calvès 2010], and ourself [Levy and Villaret 2010] have independently found direct quadratic nominal unification algorithms based on the Paterson and Wegman’s linear first-order unification algorithm [Paterson and Wegman 1978].

The use of  $\alpha$ -equivalence and binders in nominal logic immediately suggests to look at nominal unification from a higher-order perspective, the one that we adopt in this paper. Some intuitions about this relation were already roughly described by Urban, Pitts and Gabbay in [Urban et al. 2004]. Cheney [Cheney 2005b] reduces higher-order pattern unification to nominal unification (here we prove the opposite reduction).

The main benefit of nominal logic, compared to higher-order logic, is that it allows the use of binding and  $\alpha$ -equivalence without the other difficulties associated with the  $\lambda$ -calculus. In particular, with respect to unification, we have that nominal unification is unitary (most general unifiers are unique) and decidable [Urban et al. 2003; 2004], whereas higher-order unification is undecidable and infinitary [Lucchesi 1972; Goldfarb 1981; Levy 1998; Levy and Veanes 2000]. In this paper we fully develop the study of nominal unification from the higher-order logics’ view. We

show that *full* higher-order unification is not needed, and *Higher-order Pattern Unification* suffices to encode Nominal Unification. This subclass of problems was introduced by Miller [Miller 1991]. Contrarily to general higher-order unification, higher-order pattern unification is decidable and unitary [Miller 1991; Nipkow 1993]. Moreover, unifiability can be decided in linear time [Qian 1996]. All this will lead us to show how to reduce nominal unification to higher-order pattern unification, and to conclude its decidability in quadratic deterministic time.

From a higher-order perspective, nominal unification can be seen as a variant of higher-order unification where:

- (1) variables are all first-order typed, and constants are of order at most three,
- (2) unification is performed modulo  $\alpha$ -equivalence, instead of the usual  $\alpha$  and  $\beta$ -equivalence,
- (3) instances of variables are allowed to capture atoms, contrarily to the standard higher-order definition, and
- (4) apart from the usual equality predicate, we use a *freshness* predicate  $a \# t$  with the intended meaning: atom  $a$  does not occur free in  $t$ .

The third point is the key that makes nominal unification an interesting subject of research. Variable capture is always a trouble spot. Roughly speaking, the main idea of this paper is to translate atoms into bound variables, and variables into free variables with the list of atoms that they can *capture* as arguments. The first point will ensure that, since variables do not have parameters, after translation, the only arguments of free variables will be list of pairwise distinct bound variables, hence higher-order patterns. Moreover, since bound variables will be first-order typed, and constants third-order typed, the translated problems will be *second-order* patterns. The second point is not a difficulty. Since all nominal variables are first-order typed, their instantiation does not introduce  $\beta$ -redexes. Finally, the fourth point can also be overcome by translating freshness equations into equality equations, as described in Section 4.

The remainder of the paper proceeds as follows. After some preliminaries in Section 2, in Section 3 we illustrate by examples the main ideas of the reduction at the same time that we show the main features of nominal unification. In Section 4, we prove that freshness equations can be linearly translated into equality equations. In Section 5, we show how to translate a nominal unification problem into a higher-order patterns unification problem. Then, after proving some properties of Higher-Order Pattern Unification in Section 6, we prove that this translation is effectively a quadratic time reduction, in Section 7. In Section 8, we establish a correspondence between nominal unifiers and pattern unifiers of the translated problems. In particular, we prove that the translation function and its inverse are monotone w.r.t. the more general relation, and both translate most general unifiers into most general unifiers. We conclude in Section 9.

## 2. PRELIMINARIES

In this section we present some basic definitions of Nominal Unification and Higher-Order Pattern Unification. We will use two distinct typographic fonts to represent nominal terms and  $\lambda$ -terms along this paper.

## 2.1 Nominal Unification

Nominal terms contain *variables* and *atoms*. Only variables may be instantiated, and only atoms may be bounded. They roughly correspond to the notions of free and bound variables in  $\lambda$ -calculus, respectively, but are considered as completely different entities. However, atoms are not necessarily bounded, and when they occur free, they are not instantiable.

In *nominal signatures* we have *sorts of atoms* (typically  $\nu$ ) and *sorts of data* (typically  $\delta$ ) as disjoint sets. *Atoms* (typically  $a, b, \dots$ ) have one of the sorts of atoms. *Variables*, also called *unknowns*, (typically  $X, Y, \dots$ ) have a sort of atom or sort of data, i.e. of the form  $\nu \mid \delta$ . *Nominal function symbols* (typically  $f, g, \dots$ ) have an *arity* of the form  $\tau_1 \times \dots \times \tau_n \rightarrow \delta$ , where  $\delta$  is a sort of data and  $\tau_i$  are sorts given by the grammar  $\tau ::= \nu \mid \delta \mid \langle \nu \rangle \tau$ . Abstractions have sorts of the form  $\langle \nu \rangle \tau$ .

*Nominal terms* (typically  $t, u, \dots$ ) are given by the grammar:

$$t ::= f(t_1, \dots, t_n) \mid a \mid a.t \mid \pi.X$$

where  $f$  is a  $n$ -ary function symbol,  $a$  is an atom,  $\pi$  is a permutation (finite list of swappings), and  $X$  is a variable. They are called respectively *application*, *atom*, *abstraction* and *suspension*. The set of variables of a term  $t$  is denoted by  $\text{Vars}(t)$ .

A *swapping*  $(ab)$  is a pair of atoms of the same sort. The effect of a swapping over an atom is defined by  $(ab) \cdot a = b$  and  $(ab) \cdot b = a$  and  $(ab) \cdot c = c$ , when  $c \neq a, b$ . For the rest of terms the extension is straightforward, in particular,  $(ab) \cdot (c.t) = ((ab) \cdot c) \cdot ((ab) \cdot t)$ . A *permutation* is a (possibly empty) sequence of swappings. Its effect is defined by  $(a_1 b_1) \dots (a_n b_n) \cdot t = (a_1 b_1) \cdot ((a_2 b_2) \dots (a_n b_n) \cdot t)$ . Notice that every permutation  $\pi$  naturally defines a bijective function from the set of atoms to the sets of atoms, that we will also represent as  $\pi$ . *Suspensions* are uses of variables with a permutation of atoms waiting to be applied once the variable is instantiated. Occurrences of an atom  $a$  are said to be *bound* if they are in the scope of an abstraction of  $a$ , otherwise are said to be *free*.

*Substitutions* are finite sets of pairs  $[X_1 \mapsto t_1, \dots, X_n \mapsto t_n]$  where  $X_i$  and  $t_i$  have the same sort, and the  $X_i$ 's are pairwise distinct variables. They can be extended to sort-respecting functions between terms, and behave like in first-order logic, hence allowing atom capture. For instance  $[X \mapsto a]a.X = a.a$ . Remember that when applying a substitution to a suspension, the permutation is immediately applied, for instance

$$[X \mapsto g(a)]f((ab) \cdot X, X) = f((ab) \cdot g(a), g(a)) = f(g((ab) \cdot a), g(a)) = f(g(b), g(a))$$

The domain of a substitution  $\sigma = [X_1 \mapsto t_1, \dots, X_n \mapsto t_n]$  is  $\text{Dom}(\sigma) = \{X_1, \dots, X_n\}$ . For convenience we consider  $\text{Dom}([X \mapsto X]) = \{X\} \neq \{Y\} = \text{Dom}([Y \mapsto Y])$ , although both substitutions have the same effect when applied to any term.<sup>1</sup> Composition of substitutions is defined by  $\sigma_1 \circ \sigma_2 = [X \mapsto \sigma_1(\sigma_2(X)) \mid X \in \text{Dom}(\sigma_1) \cup \text{Dom}(\sigma_2)]$ . The restriction of a substitution  $\sigma$  to a set of variables  $V$ , written  $\sigma|_V$ , is defined as  $\sigma|_V = [X \mapsto \sigma(X) \mid X \in V]$ .

A *freshness environment* (typically  $\nabla$ ) is a list of *freshness constraints*  $a \# X$  stating that the instantiation of  $X$  cannot contain free occurrences of  $a$ .

<sup>1</sup>We have adopted this definition motivated by Remark 5.9.

The notion of  $\alpha$ -equivalence between terms, noted  $\approx$ , is defined by means of the following theory:

$$\begin{array}{c}
\frac{}{\nabla \vdash a \approx a} \text{ (\approx-atom)} \qquad \frac{a \# X \in \nabla \text{ for all } a \text{ such that } \pi \cdot a \neq \pi' \cdot a}{\nabla \vdash \pi \cdot X \approx \pi' \cdot X} \text{ (\approx-susp.)} \\
\\
\frac{\nabla \vdash t_1 \approx t'_1 \quad \dots \quad \nabla \vdash t_n \approx t'_n}{\nabla \vdash f(t_1, \dots, t_n) \approx f(t'_1, \dots, t'_n)} \text{ (\approx-application)} \\
\\
\frac{\nabla \vdash t \approx t'}{\nabla \vdash a.t \approx a.t'} \text{ (\approx-abst-1)} \qquad \frac{a \neq a' \quad \nabla \vdash t \approx (a a') \cdot t' \quad \nabla \vdash a \# t'}{\nabla \vdash a.t \approx a'.t'} \text{ (\approx-abst-2)}
\end{array}$$

where the *freshness* predicate  $\#$  is defined by:

$$\begin{array}{c}
\frac{a \neq a'}{\nabla \vdash a \# a'} \text{ (\#-atom)} \qquad \frac{(\pi^{-1} \cdot a \# X) \in \nabla}{\nabla \vdash a \# \pi \cdot X} \text{ (\#-susp.)} \\
\\
\frac{\nabla \vdash a \# t_1 \quad \dots \quad \nabla \vdash a \# t_n}{\nabla \vdash a \# f(t_1, \dots, t_n)} \text{ (\#-application)} \\
\\
\frac{}{\nabla \vdash a \# a.t} \text{ (\#-abst-1)} \qquad \frac{a \neq a' \quad \nabla \vdash a \# t}{\nabla \vdash a \# a'.t} \text{ (\#-abst-2)}
\end{array}$$

Their intended meanings are:

- $\nabla \vdash a \# t$  holds if, for every substitution  $\sigma$  respecting the freshness environment  $\nabla$  (i.e. avoiding the atom captures forbidden by  $\nabla$ ),  $a$  is not free in  $\sigma(t)$ ;
- $\nabla \vdash t \approx u$  holds if, for every substitution  $\sigma$  respecting the freshness environment  $\nabla$ ,  $t$  and  $u$  are  $\alpha$ -equivalent.

A *nominal unification problem* (typically  $P$ ) is a set of equations of the form  $t \stackrel{?}{\approx} u$ , or of the form  $a \stackrel{?}{\#} t$ , called *equality equations* and *freshness equations*, respectively.

A *solution* or *unifier* of a nominal problem  $P$  is a pair  $\langle \nabla, \sigma \rangle$  satisfying  $\nabla \vdash a \# \sigma(t)$ , for all freshness equations  $a \stackrel{?}{\#} t \in P$ , and  $\nabla \vdash \sigma(t) \approx \sigma(u)$ , for all equality equations  $t \stackrel{?}{\approx} u \in P$ . Later, in Section 5, we will also require solutions to satisfy  $\text{Dom}(\sigma) = \text{Vars}(P)$ . In Remark 5.9 we justify why this does not affect to solvability of nominal problems.

Given two substitutions  $\sigma_1$  and  $\sigma_2$ , and two freshness environments  $\nabla_1$  and  $\nabla_2$ , we say that  $\nabla_2 \vdash \sigma_1(\nabla_1)$ , if  $\nabla_2 \vdash a \# \sigma_1(X)$  holds for each  $a \# X \in \nabla_1$ ; and we say that  $\nabla_1 \vdash \sigma_1 \approx \sigma_2$ , if  $\nabla_1 \vdash \sigma_1(X) \approx \sigma_2(X)$  holds for all  $X \in \text{Dom}(\sigma_1) \cup \text{Dom}(\sigma_2)$ . Given a nominal unification problem  $P$ , we say that a solution  $\langle \nabla_1, \sigma_1 \rangle$  is *more general* than another solution  $\langle \nabla_2, \sigma_2 \rangle$ , if there exists a substitution  $\sigma'$  satisfying  $\nabla_2 \vdash \sigma'(\nabla_1)$  and  $\nabla_2 \vdash \sigma' \circ \sigma_1|_{\text{Dom}(\sigma_1) \cup \text{Dom}(\sigma_2)} \approx \sigma_2$ . As usual, we say that a solution  $\sigma$  is *most general* if, for any other solution  $\sigma'$  more general than  $\sigma$ , we have also that  $\sigma$  is also more general than  $\sigma'$ . Most general nominal unifiers are *unique*, in

the usual sense: if  $\sigma_1$  and  $\sigma_2$  are both most general, then  $\sigma_1$  is more general than  $\sigma_2$ , and vice versa.

EXAMPLE 2.1. The solutions of the equation  $\mathbf{a}.X \stackrel{?}{\approx} \mathbf{b}.Y$  can not instantiate  $X$  with terms containing free occurrences of the atom  $\mathbf{b}$ , for instance if we apply the substitution  $[X \mapsto \mathbf{b}]$  to both sides of the equation we get  $[X \mapsto \mathbf{b}](\mathbf{a}.X) = \mathbf{a}.\mathbf{b}$ , for the left hand side, and  $[X \mapsto \mathbf{b}](\mathbf{b}.Y) = \mathbf{b}.Y$ , for the right hand side, and obviously  $\mathbf{a}.\mathbf{b} \stackrel{?}{\approx} \mathbf{b}.Y$  is unsolvable.

A most general solution of this equation is  $\langle \{\mathbf{b}\#X\}, Y \mapsto (\mathbf{a}\mathbf{b}) \cdot X \rangle$ . Another most general solution is  $\langle \{\mathbf{a}\#Y\}, [X \mapsto (\mathbf{a}\mathbf{b}) \cdot Y] \rangle$ . Notice that the first unifier is equal to the second composed with  $\sigma' = [Y \mapsto (\mathbf{a}\mathbf{b}) \cdot X]$ , hence the second one is more general than the first one. Similarly, the first one is more general than the second one. Hence, both are equivalent.

## 2.2 Higher-Order Pattern Unification

In higher-order signatures we have *types* constructed from a set of *basic types* (typically  $\delta, \nu, \dots$ ) using the grammar  $\tau ::= \delta \mid \nu \mid \tau \rightarrow \tau$ , where  $\rightarrow$  is associative to the right. *Variables* (typically  $X, Y, Z, x, y, z, a, b, \dots$ ) and *constants* (typically  $f, c, \dots$ ) have an assigned type.

$\lambda$ -terms are built using the grammar

$$t ::= x \mid c \mid \lambda x.t \mid t_1 t_2$$

where  $x$  is a variable and  $c$  is a constant, and are typed as usual. For convenience, terms of the form  $(\dots (a t_1) \dots t_n)$ , where  $a$  is a constant or a variable, will be written as  $a(t_1, \dots, t_n)$ , and terms of the form  $\lambda x_1. \dots \lambda x_n. t$  as  $\lambda x_1, \dots, x_n. t$ . We use  $\vec{x}$  as a short-hand for  $x_1, \dots, x_n$ . If nothing is said, terms are assumed to be written in  $\eta$ -long  $\beta$ -normal form. Therefore, all terms have the form  $\lambda x_1. \dots \lambda x_n. h(t_1, \dots, t_m)$ , where  $m, n \geq 0$ ,  $h$  is either a constant or a variable,  $t_1, \dots, t_m$  have also this form, and the term  $h(t_1, \dots, t_m)$  has a basic type.

Other standard notions of the simply typed  $\lambda$ -calculus, like *bound* and *free* occurrences of variables,  $\alpha$ -conversion,  $\beta$ -reduction,  $\eta$ -long  $\beta$ -normal form, etc. are defined as usual (see [Dowek 2001]). We will notate free occurrences of variables with capital letters  $X, Y, \dots$ , for the sake of readability. The set of free variables of a term  $t$  is denoted by  $\text{Vars}(t)$ . When we write an equality between two  $\lambda$ -terms, we mean that they are equivalent modulo  $\alpha$ ,  $\beta$  and  $\eta$  equivalence. When we write an equality  $=_\alpha$ , we mean that they are  $\alpha$ -equivalent.

*Substitutions* are finite sets of pairs  $\sigma = [X_1 \mapsto t_1, \dots, X_n \mapsto t_n]$  where  $X_i$  and  $t_i$  have the same type and the  $X_i$ 's are pairwise distinct variables. They can be extended to type preserving function from terms to terms as usual. The *domain* is  $\text{Dom}(\sigma) = \{X_1, \dots, X_n\}$ . We say that a substitution  $\sigma_1$  is *more general* than another substitution  $\sigma_2$ , if there exists a substitution  $\sigma'$  satisfying  $\sigma' \circ \sigma_1(X) = \sigma_2(X)$ , for all  $X \in \text{Dom}(\sigma_1) \cup \text{Dom}(\sigma_2)$ . We say that a variable  $X$  *occurs* in a substitution  $\sigma$ , if  $X \in \text{Vars}(\sigma(Y))$ , for some  $Y \in \text{Dom}(\sigma)$ .

A *higher-order unification problem* is a finite set of equations  $P = \{t_1 \stackrel{?}{=} u_1, \dots, t_n \stackrel{?}{=} u_n\}$ , where  $t_i$  and  $u_i$  have the same type. A *solution* or *unifier* of a unification problem  $P$  is a substitution  $\sigma$  satisfying  $\sigma(t) = \sigma(u)$ , for all equations  $t \stackrel{?}{=} u \in P$ . We say that a unifier  $\sigma$  is *most general* if, for any other unifier  $\sigma'$  more

general than  $\sigma$ , we have  $\sigma$  is also more general than  $\sigma'$ .

A *higher-order pattern* is a  $\lambda$ -term where, when written in  $\beta\eta$ -normal form, all free variable occurrences are applied to lists of pairwise distinct bound variables. For instance,  $\lambda x.f(X(x), Y)$ ,  $f(c, \lambda x.x)$  and  $\lambda x, y.X(\lambda z.x(z), y)$  are patterns, while  $\lambda x.f(X(X(x)), Y)$ ,  $f(X(c), c)$  and  $\lambda x.\lambda y.X(x, x)$  are not. Notice that, since  $\lambda z.x(z)$  is equivalent to  $x$ , the parameters of  $X(\lambda z.x(z), y)$  are considered a list of pairwise distinct bound variables.

*Higher-order pattern unification* is the problem of deciding if there exists a unifier for a set of equations between higher-order patterns. Like in nominal unification, most general pattern unifiers are unique. Moreover, most general unifiers instantiate variables by higher-order patterns.

The following is a set of rules defining Nipkow's algorithm [Nipkow 1993] that computes, when it exists, the most general unifier of a pattern unification problem.

$$\begin{aligned}
\lambda x.s &\stackrel{?}{=} \lambda x.t \rightarrow \langle \{s \stackrel{?}{=} t\}, [\ ] \rangle \\
a(t_1, \dots, t_n) &\stackrel{?}{=} a(u_1, \dots, u_n) \rightarrow \langle \{t_1 \stackrel{?}{=} u_1, \dots, t_n \stackrel{?}{=} u_n\}, [\ ] \rangle \\
&\text{where } a \text{ is a constant or bound variable} \\
Y(\vec{x}) &\stackrel{?}{=} a(u_1, \dots, u_m) \rightarrow \langle \{Y_1(\vec{x}) \stackrel{?}{=} u_1, \dots, Y_m(\vec{x}) \stackrel{?}{=} u_m\}, \\
&\quad [Y \mapsto \lambda \vec{x}.a(Y_1(\vec{x}), \dots, Y_m(\vec{x}))]\rangle \\
&\text{where } Y \notin \text{FV}(u_1, \dots, u_m) \\
&\text{and } a \text{ is a constant or } a \in \{\vec{x}\} \\
X(\vec{x}) &\stackrel{?}{=} X(\vec{y}) \rightarrow \langle \emptyset, [X \mapsto \lambda \vec{x}.Z(\vec{z})] \rangle \\
&\text{where } \{\vec{z}\} = \{x_i \mid x_i = y_i\} \\
X(\vec{x}) &\stackrel{?}{=} Y(\vec{y}) \rightarrow \langle \emptyset, [X \mapsto \lambda \vec{x}.Z(\vec{z}), Y \mapsto \lambda \vec{y}.Z(\vec{z})] \rangle \\
&\text{where } X \neq Y \text{ and } \{\vec{z}\} = \{\vec{x}\} \cap \{\vec{y}\}
\end{aligned}$$

The rules transform any equation into a pair  $\langle \text{set of equations, substitution} \rangle$ . The algorithm proceeds by replacing the equation on the left of the rule by the set of equations on the right. The substitution is applied to the new set of equations, and used to, step by step, construct the unifier. Therefore, any rule of the form  $t \stackrel{?}{=} u \rightarrow \langle E, \rho \rangle$  produces a transformation of the form

$$\langle P \cup \{t \stackrel{?}{=} u\}, \sigma \rangle \Rightarrow \langle \rho(P) \cup E, \rho \circ \sigma \rangle$$

The algorithm starts with the pair  $\langle P, Id \rangle$  and, if  $P$  is solvable, finishes with  $\langle \emptyset, \sigma \rangle$ , where  $\sigma$  with domain restricted to  $\text{FV}(P)$  is the most general unifier [Nipkow 1993, Theorem 3.1].

In the first rule the binder can be removed because, in Nipkow's presentation, free and bound variable names are assumed to be from distinct sets, and can be distinguished. The equations on the right of the second rule may not be normalized, i.e. the term  $\lambda \vec{x}.Y_i(x_1, \dots, x_n)$  may require a  $\eta$ -expansion when  $u_i$  is not base typed.

There is an algorithm that finds higher-order pattern unifiers, if exist, in linear time [Qian 1996].

### 3. FOUR EXAMPLES

In order to describe the reduction of nominal unification to higher-order pattern unification, we will use the unification problems proposed in [Urban et al. 2003; 2004] as a quiz.

EXAMPLE 3.1. The nominal equation

$$\mathbf{a}.\mathbf{b}.f(\mathbf{X}_1, \mathbf{b}) \stackrel{?}{\approx} \mathbf{b}.\mathbf{a}.f(\mathbf{a}, \mathbf{X}_1)$$

has no nominal unifiers. Notice that, although unification is performed modulo  $\alpha$ -equivalence, as far as we allow atom capture, we can not  $\alpha$ -convert terms before instantiating them. Therefore, this problem is *not* equivalent to

$$\mathbf{a}.\mathbf{b}.f(\mathbf{X}_1, \mathbf{b}) \stackrel{?}{\approx} \mathbf{a}.\mathbf{b}.f(\mathbf{b}, \mathbf{X}_1)$$

which is solvable, and must be  $\alpha$ -converted as

$$\mathbf{a}.\mathbf{b}.f(\mathbf{X}_1, \mathbf{b}) \stackrel{?}{\approx} \mathbf{a}.\mathbf{b}.f(\mathbf{b}, (\mathbf{a} \ \mathbf{b}) \cdot \mathbf{X}_1)$$

Recall that  $(\mathbf{a} \ \mathbf{b}) \cdot \mathbf{X}_1$  means that, after instantiating  $\mathbf{X}_1$  with a term that possibly contain  $\mathbf{a}$  or  $\mathbf{b}$ , we have to exchange these variables.

According to the ideas exposed in the introduction, we have to replace every occurrence of  $\mathbf{X}_1$  by  $X_1(a, b)$ , since  $\langle \mathbf{a}, \mathbf{b} \rangle$  is the list of atoms (bound variables  $a, b$ ) that can be captured. We get:

$$\lambda a.\lambda b.f(X_1(a, b), b) \stackrel{?}{=} \lambda b.\lambda a.f(a, X_1(a, b))$$

Since this is a higher-order unification problem, we can  $\alpha$ -convert one of the sides of the equation and get:

$$\lambda a.\lambda b.f(X_1(a, b), b) \stackrel{?}{=} \lambda a.\lambda b.f(b, X_1(b, a))$$

which is unsolvable, like the original nominal equation.

EXAMPLE 3.2. The nominal equation

$$\mathbf{a}.\mathbf{b}.f(\mathbf{X}_2, \mathbf{b}) \stackrel{?}{\approx} \mathbf{b}.\mathbf{a}.f(\mathbf{a}, \mathbf{X}_3)$$

is solvable. Its translation is

$$\lambda a.\lambda b.f(X_2(a, b), b) \stackrel{?}{=} \lambda b.\lambda a.f(a, X_3(a, b))$$

The most general unifier of this higher-order pattern unification problem is

$$\begin{aligned} X_2 &\mapsto \lambda x.\lambda y.y \\ X_3 &\mapsto \lambda x.\lambda y.x \end{aligned}$$

Now, taking into account that the first argument corresponds to the atom  $\mathbf{a}$ , and the second one to  $\mathbf{b}$ , we can reconstruct the most general nominal unifier as:

$$\begin{aligned} \mathbf{X}_2 &\mapsto \mathbf{b} \\ \mathbf{X}_3 &\mapsto \mathbf{a} \end{aligned}$$

EXAMPLE 3.3. In some cases, there are interrelationships between the instances of variables that make reconstruction of unifiers more difficult. This is shown with the following example:

$$\mathbf{a}.\mathbf{b}.f(\mathbf{b}, \mathbf{X}_4) \stackrel{?}{\approx} \mathbf{b}.\mathbf{a}.f(\mathbf{a}, \mathbf{X}_5)$$

that is solvable. Its translation results on:

$$\lambda a.\lambda b.f(b, X_4(a, b)) \stackrel{?}{=} \lambda b.\lambda a.f(a, X_5(a, b))$$



and its most general unifier is:<sup>2</sup>

$$X_4 \mapsto \lambda x. \lambda y. X_5(y, x)$$

This higher-order unifier can be used to reconstruct the nominal unifier

$$X_4 \mapsto (a \ b) \cdot X_5$$

The swapping  $(a \ b)$  comes from the fact that the arguments of  $X_5$  and the lambda abstractions in front have a different order.

EXAMPLE 3.4. The solution of a nominal unification problem is not just a substitution, but a pair  $\langle \nabla, \sigma \rangle$  where  $\sigma$  is a substitution and  $\nabla$  is a freshness environment imposing some restrictions on the atoms that can occur free in the fresh variables introduced by  $\sigma$ . The nominal equation

$$a.b.f(b, X_6) \stackrel{?}{\approx} a.a.f(a, X_7)$$

has as solution

$$\begin{aligned} \sigma &= [X_6 \mapsto (b \ a) \cdot X_7] \\ \nabla &= \{b \# X_7\} \end{aligned}$$

where the freshness environment is not empty and requires instances of  $X_7$  to not contain (free) occurrences of  $b$ . Let us see how this is reflected when we translate the problem into a higher-order unification problem. The translation of the equation using the translation algorithm results on:

$$\lambda a. \lambda b. f(b, X_6(a, b)) \stackrel{?}{=} \lambda a. \lambda a. f(a, X_7(a, b)) \quad (1)$$

After a convenient  $\alpha$ -conversion we get

$$\lambda a. \lambda c. f(c, X_6(a, c)) \stackrel{?}{=} \lambda a. \lambda c. f(c, X_7(c, b))$$

The most general unifier is again unique:

$$\begin{aligned} X_6 &\mapsto \lambda x. \lambda y. X_8(y, b) \\ X_7 &\mapsto \lambda x. \lambda y. X_8(x, y) \end{aligned}$$

Nevertheless, in this case we cannot reconstruct the nominal unifier. Moreover, by instantiating the free variable  $b$ , we get other (non-most general) higher-order unifier without nominal counterpart. The translation does not work in this case because  $b$  occurs free in the right hand side of (1). We translate both atoms and nominal variables as higher-order variables. Occurrences of nominal variables become free occurrences of variables, and occurrences of atoms, if are bounded, become bound occurrences of variables. Therefore, in most cases, after the translation the distinction atom/variable become a distinction free/bound variable. However, if atoms are not bounded, as in this case, they are translated as free variables, hence are instantiable, whereas atoms are not instantiable.

To avoid this problem, we have to ensure that any occurrence of an atom is translated as a bound variable occurrence. This is easily achievable if we add

<sup>2</sup>The unifier  $X_5 \mapsto \lambda x. \lambda y. X_4(y, x)$  is equivalent modulo variable renaming. In this case we obtain the also equivalent nominal unifier  $X_5 \mapsto (a \ b) \cdot X_4$ .

binders in front of both sides of the equation. Therefore, the correct translation of this problem is:

$$\lambda a. \lambda b. \lambda a. \lambda b. f(b, X_6(a, b)) \stackrel{?}{=} \lambda a. \lambda b. \lambda a. \lambda a. f(a, X_7(a, b))$$

where two new binder  $\lambda a. \lambda b$  have been introduced in front of both sides of the equation. The most general unifier is now:

$$\begin{aligned} X_6 &\mapsto \lambda x. \lambda y. X_8(y) \\ X_7 &\mapsto \lambda x. \lambda y. X_8(x) \end{aligned}$$

This can be used to reconstruct the nominal substitution:

$$\begin{aligned} X_6 &\mapsto (a \ b) \cdot X_8 \\ X_7 &\mapsto X_8 \end{aligned}$$

As far as  $X_8(x)$  is translated back as  $X_8$ , and  $X_8(x)$  does not uses the second argument (the one corresponding to  $b$ ), we have to add a supplementary condition ensuring that  $X_8$  does not contain free occurrences of  $b$ . This results on the freshness environment  $\{b \# X_8\}$ . Then,  $X_8(y)$  is translated back as  $(a \ b) \cdot X_8$ .

#### 4. REMOVING FRESHNESS EQUATIONS

In this section we show that freshness equations do not contribute to make nominal unification more expressive. We prove that nominal unification can be linearly-reduced to nominal unification without freshness equations. We call this restriction of nominal unification *equational nominal unification*. In next sections we will describe a quadratic reduction of equational nominal unification to higher-order pattern unification. The absence of freshness equations makes the reduction to higher-order pattern unification simpler, compared with the reduction described in the preliminary version of this paper [Levy and Villaret 2008].

**DEFINITION 4.1.** *We define the translation of nominal unification problems into equational nominal unification problems inductively as follows:*

$$\begin{aligned} Eq(\{a \# ?t\} \cup P) &= \{a.b.t \stackrel{?}{\approx} b.b.t\} \cup Eq(P) \text{ for some } b \neq a \\ Eq(\{t \stackrel{?}{\approx} u\} \cup P) &= \{t \stackrel{?}{\approx} u\} \cup Eq(P) \end{aligned}$$

**LEMMA 4.2.** *Given a nominal unification problem  $P$ , its translation into equational nominal unification  $Eq(P)$  can be calculated in linear time. Hence,  $Eq(P)$  has linear-size on the size of  $P$ .*

**LEMMA 4.3.** *The pair  $\langle \nabla, \sigma \rangle$  solves  $P$ , if, and only if,  $\langle \nabla, \sigma \rangle$  solves  $Eq(P)$ .*

**PROOF.** We first prove that  $\langle a \# t, Id \rangle$  is a solution of  $\{a.b.t \stackrel{?}{\approx} b.b.t\}$  when  $b \neq a$

$$\frac{\frac{\frac{t \approx t \quad b \# (a \ b) \cdot t}{b.t \approx a.(a \ b) \cdot t} \quad (\approx\text{-abst-2}) \quad \frac{a \# t}{a \# b.t} \quad (\# \text{-abst-2})}{a.b.t \approx b.b.t} \quad (\approx\text{-abst-2})$$

(lemma 2.7)

In this proof we prove  $t \approx t$  from an empty set of assumptions. We can prove that this is always possible, for any term  $t$ , by structural induction on  $t$ . We also prove  $b\#(a\ b) \cdot t$  from  $a\#t$ , using Lemma 2.7 of [Urban et al. 2004].

Lemma 2.14 of [Urban et al. 2004] states that  $\nabla' \vdash \sigma(\nabla)$  and  $\nabla \vdash t \approx t'$  implies  $\nabla' \vdash \sigma(t) \approx \sigma(t')$ . In particular,  $\nabla \vdash \sigma(a\#t)$  and  $a\#t \vdash a.b.t \approx b.b.t$  implies  $\nabla \vdash \sigma(a.b.t) \approx \sigma(b.b.t)$ . Therefore, if  $\langle \nabla, \sigma \rangle$  solves  $a\#^?t$ , then  $\langle \nabla, \sigma \rangle$  solves  $a.b.t \approx^? b.b.t$ .

Second, analyzing the previous proof, we see that the inference rules applied in each situation were the only applicable rules. Therefore, any solution  $\langle \nabla, \sigma \rangle$  solving  $a.b.t \approx^? b.b.t$ , also solves  $a\#^?t$ , because any proof of  $\sigma(a.b.t) \approx \sigma(b.b.t)$  contains a proof of  $a\#\sigma(t)$  as a sub-proof.

From, these two facts we conclude that  $a\#^?t$  and  $a.b.t \approx^? b.b.t$  have the same set of solutions, for any  $b \neq a$ . Therefore,  $\{a\#^?t\} \cup P$  and  $\{a.b.t \approx^? b.b.t\} \cup P$ , also have the same set of solutions, for any nominal unification problem  $P$ . From this we conclude that  $P$  and  $Eq(P)$  have the same set of solutions.  $\square$

**COROLLARY 4.4.** *Nominal unification can be linearly-reduced to equational nominal unification.*

## 5. THE TRANSLATION ALGORITHM

In this section we formalize the translation algorithm. We transform equational nominal unification problems into higher-order unification problems. Both kinds of problems are expressed using distinct kinds of signatures. In nominal unification we have sorts of atoms and sorts of data. In higher-order this distinction is no longer necessary, and we will have a *base type* for every sort of atoms  $\nu$  or sort of data  $\delta$ . We give a *sort to types translation function* that allows us to translate any sort into a type.

**DEFINITION 5.1.** *The translation function is defined on sorts inductively as follows.*

$$\begin{aligned} \llbracket \delta \rrbracket &= \delta \\ \llbracket \nu \rrbracket &= \nu \\ \llbracket \tau_1 \times \cdots \times \tau_n \rightarrow \tau \rrbracket &= \llbracket \tau_1 \rrbracket \rightarrow \cdots \rightarrow \llbracket \tau_n \rrbracket \rightarrow \llbracket \tau \rrbracket \\ \llbracket \langle \nu \rangle \tau \rrbracket &= \nu \rightarrow \llbracket \tau \rrbracket \end{aligned}$$

where  $\delta$  and  $\nu$  are base types.

**REMARK 5.2.** *The translation function for terms depends on all the atoms occurring in the nominal unification problem. We assume that there exists a fixed, finite and ordered list of distinct atoms  $\langle a_1, \dots, a_n \rangle$  used in the problem. This seems to contradict the assumption of a countably infinite set of atoms for every sort. However, this does not imply a loss of generality as far as every nominal unification problem only contains a finite set of atoms, and its solutions can be expressed without adding new atoms (this is a consequence of Lemma 6.11). Notice also that the nominal unification algorithm in [Urban et al. 2004] generates unifiers that do not introduce new atoms, because, in all transformation rules, the set of atoms in the right-hand side are a subset of the set of atoms in the left-hand side.*

*From now on, we will consider this list given and fixed.*

*In [Dowek et al. 2009; 2010] they solve this problem using a permission set for every variable. They roughly correspond to the set of atoms capturable by this*

variable. However, in their case, this set is infinite and co-infinite. In our case, we prove that solutions can be expressed using the same finite set of atoms occurring in the problem, and the set of capturable atoms of a variable is finite and co-finite.

For every function symbol  $f$ , we will use a constant with the same name  $f$ . Every atom  $a$  is translated as a (bound) variable, with the same name  $a$ . For every variable (unknown)  $X$ , we will use a (free) variable with the same name  $X$ . Trivially, atom abstractions  $a.t$  are translated as lambda abstractions  $\lambda a.t$ , and applications  $f(t_1, \dots, t_n)$  as applications  $f(t_1, \dots, t_n)$ . The translation of suspensions  $\pi.X$  is more complicated, as far as it gets rid of atom capture. Recall that in all cases we use distinct character fonts for symbols of nominal logic and symbols of the higher-order framework. The translation is parametric on a freshness environment. Notice that, although we have removed freshness equations, nominal unifiers are composed by a freshness environment and a substitution.

**DEFINITION 5.3.** *Let  $\langle a_1, \dots, a_n \rangle$  be a fixed ordered list of atoms. The translation function from nominal terms with a freshness environments  $\nabla$  into  $\lambda$ -terms is defined inductively as follows.*

$$\begin{aligned} \llbracket a \rrbracket_{\nabla} &= a \\ \llbracket f(t_1, \dots, t_n) \rrbracket_{\nabla} &= f(\llbracket t_1 \rrbracket_{\nabla}, \dots, \llbracket t_n \rrbracket_{\nabla}) \\ \llbracket a.t \rrbracket_{\nabla} &= \lambda a. \llbracket t \rrbracket_{\nabla} \\ \llbracket \pi.X \rrbracket_{\nabla} &= X(\llbracket \pi.b_1 \rrbracket_{\nabla}, \dots, \llbracket \pi.b_m \rrbracket_{\nabla}) \quad \text{where } \langle b_1, \dots, b_m \rangle = \langle a \in \langle a_1, \dots, a_n \rangle \mid a \# X \notin \nabla \rangle \end{aligned}$$

where, for any atom  $a : \nu$ ,  $a : \llbracket \nu \rrbracket$  is the corresponding bound variable, for any function symbol  $f : \tau$ ,  $f : \llbracket \tau \rrbracket$  is the corresponding constant, and for any variable  $X : \tau$ , the list  $\langle b_1, \dots, b_m \rangle$  is the sublist<sup>3</sup> of  $\langle a_1, \dots, a_n \rangle$  composed by the atoms satisfying  $a \# X \notin \nabla$ , and  $X : \llbracket \nu_1 \rrbracket \rightarrow \dots \rightarrow \llbracket \nu_m \rrbracket \rightarrow \llbracket \tau \rrbracket$  is the corresponding free variable, where  $b_j : \nu_j$ .<sup>4</sup>

**LEMMA 5.4.** *For every nominal term  $t$  of sort  $\tau$ , and freshness environment  $\nabla$ ,  $\llbracket t \rrbracket_{\nabla}$  is a  $\lambda$ -term with type  $\llbracket \tau \rrbracket$ .*

**PROOF.** The proof is simple by structural induction on  $t$ . The only point that needs a more detailed explanation is the case of suspensions. Since  $a_i : \nu_i$ ,  $X : \tau$ , and  $X : \llbracket \nu_{i_1} \rrbracket \rightarrow \dots \rightarrow \llbracket \nu_{i_m} \rrbracket \rightarrow \llbracket \tau \rrbracket$ , we have  $\llbracket X \rrbracket_{\nabla} = X(\llbracket a_{i_1} \rrbracket_{\nabla}, \dots, \llbracket a_{i_m} \rrbracket_{\nabla}) : \llbracket \tau \rrbracket$ . When  $X$  is affected by a swapping  $(a_{i_j} a_{i_k})$  we also have  $\llbracket (a_{i_j} a_{i_k}).X \rrbracket_{\nabla} = X(\dots, \llbracket a_{i_{j-1}} \rrbracket_{\nabla}, \llbracket a_{i_k} \rrbracket_{\nabla}, \llbracket a_{i_{j+1}} \rrbracket_{\nabla}, \dots, \llbracket a_{i_{k-1}} \rrbracket_{\nabla}, \llbracket a_{i_j} \rrbracket_{\nabla}, \llbracket a_{i_{k+1}} \rrbracket_{\nabla}, \dots) : \llbracket \tau \rrbracket$  because the suspension is not a valid nominal term unless  $a_{i_j}$  and  $a_{i_k}$  belong to the same sort. The same applies to arbitrary permutations.  $\square$

**EXAMPLE 5.5.** Given the nominal term  $t = a.b.c.(ca)(ab).X$ , after applying the substitution  $\sigma = [X \mapsto f(a, b, c, Y)]$  we get  $\sigma(t) = a.b.c.f(b, c, a, Y)$ . Let  $\langle a, b, c \rangle$  be the (ordered) list of atoms of our problem. The translation of the term  $t$  w.r.t.  $\nabla_1 = \emptyset$  results into  $\llbracket t \rrbracket_{\nabla_1} = \lambda a. \lambda b. \lambda c. X(b, c, a)$  and, the translation of the instantiation  $\sigma(t)$  w.r.t.  $\nabla_2 = \{a \# Y\}$  results into  $\llbracket \sigma(t) \rrbracket_{\nabla_2} = \lambda a. \lambda b. \lambda c. f(b, c, a, Y(c, a))$ . There is a  $\lambda$ -substitution  $[X \mapsto \lambda a. \lambda b. \lambda c. f(a, b, c, Y(\bar{b}, c))]$  (described in Definition 5.8) that

<sup>3</sup>Notice that we say sublist, not subset, to emphasize that the relative order between  $a$ 's is preserved.

<sup>4</sup>Notice that  $b_j$  and  $\pi.b_j$  are of the same sort.

when applied to  $\llbracket t \rrbracket_{\nabla_1}$  results into  $\llbracket \sigma(t) \rrbracket_{\nabla_2}$ . Graphically this can be represented as the commutation of the following diagram (proved in Lemma 5.11).

$$\begin{array}{ccc}
 a.b.c.(ca)(ab) \cdot X & \xrightarrow{[X \mapsto f(a, b, c, Y)]} & a.b.c.f(b, c, a, (ca)(ab)) \cdot Y \\
 \downarrow \llbracket \cdot \rrbracket_{\emptyset} & & \downarrow \llbracket \cdot \rrbracket_{\{a \# Y\}} \\
 \lambda a. \lambda b. \lambda c. X(b, c, a) & \xrightarrow{[X \mapsto \lambda a. \lambda b. \lambda c. f(a, b, c, Y(b, c))]} & \lambda a. \lambda b. \lambda c. f(b, c, a, Y(c, a))
 \end{array}$$

DEFINITION 5.6. Let  $\langle a_1, \dots, a_n \rangle$  be an ordered list of atoms. The translation function is defined on equational nominal problems inductively as follows

$$\llbracket \{t \approx u\} \cup P \rrbracket = \{\lambda a_1. \dots \lambda a_n. \llbracket t \rrbracket_{\emptyset} \stackrel{?}{=} \lambda a_1. \dots \lambda a_n. \llbracket u \rrbracket_{\emptyset}\} \cup \llbracket P \rrbracket$$

LEMMA 5.7. Given an equational nominal unification problem  $P$ , its translation  $\llbracket P \rrbracket$  is a higher-order pattern unification problem.

Moreover, the size and the time needed to compute  $\llbracket P \rrbracket$  is bounded by the square of the size of  $P$ .

PROOF. By Lemma 5.4,  $\lambda a_1. \dots \lambda a_n. \llbracket t \rrbracket_{\emptyset} \stackrel{?}{=} \lambda a_1. \dots \lambda a_n. \llbracket u \rrbracket_{\emptyset}$  is an equation between  $\lambda$ -terms of the same type. Now notice that  $\llbracket \pi \cdot X \rrbracket_{\nabla} = X(\llbracket \pi \cdot b_1 \rrbracket_{\nabla}, \dots, \llbracket \pi \cdot b_m \rrbracket_{\nabla})$  translate the variable  $X$  into an application of the free variable  $X$  to a list of pairwise distinct bound variables, because the  $b_i$  are all different,  $\pi$  is a permutation, and we ensure that all atoms are translated into bound variables by adding  $\lambda$ -bindings in front of both terms. Therefore, both sides of the equation are higher-order patterns.

Concerning the size of the translation, we obtain a quadratic bound due to the translation of these suspensions.  $\square$

Finally, we have to translate solutions of nominal unification problems into  $\lambda$ -substitutions.

DEFINITION 5.8. Let  $\langle a_1, \dots, a_n \rangle$  be a fixed ordered list of atoms. Given a nominal substitution  $\sigma$ , and a freshness environment  $\nabla$ , we define the following translation function

$$\llbracket \sigma \rrbracket_{\nabla} = \bigcup_{X \in \text{Dom}(\sigma)} \left[ X \mapsto \lambda a_1. \dots \lambda a_n. \llbracket \sigma(X) \rrbracket_{\nabla} \right]$$

The following remark shows why in some places we require that solutions  $\langle \nabla, \sigma \rangle$  of a nominal problem  $P$  satisfy  $\text{Dom}(\sigma) = \text{Vars}(P)$ .

REMARK 5.9. Let  $\langle a, b \rangle$  be the fixed list of atoms.

Consider the nominal unification problem  $P_1 = \{a.X \approx b.Y\}$ , and its translations as a higher-order pattern unification problem

$$\llbracket P_1 \rrbracket = \llbracket \{a.X \approx b.Y\} \rrbracket = \{\lambda a. \lambda b. \lambda a. X(a, b) \stackrel{?}{=} \lambda a. \lambda b. \lambda b. Y(a, b)\}$$

The  $\lambda$ -substitution

$$\sigma_1 = \llbracket [X \mapsto (a\ b) \cdot Y] \rrbracket_{\{a \# Y\}} = [X \mapsto \lambda a. \lambda b. Y(a)]$$

does not solve  $\llbracket P_1 \rrbracket$ . Whereas the  $\lambda$ -substitution

$$\sigma_2 = \llbracket [X \mapsto (a\ b) \cdot Y, Y \mapsto Y] \rrbracket_{\{a \# Y\}} = [X \mapsto \lambda a. \lambda b. Y(a), Y \mapsto \lambda a. \lambda b. Y(b)]$$

solves  $\llbracket P_1 \rrbracket$ . Notice that in the first case the domain of the nominal unifier (as defined in Section 2) is  $\{X\}$ , whereas in the other case it is  $\{X, Y\} = \text{Vars}(P_1)$ .

We will see (Theorem 5.13) that, if  $\text{Vars}(P) \subseteq \text{Dom}(\sigma)$  and  $\langle \nabla, \sigma \rangle$  solves  $P$ , then  $\llbracket \sigma \rrbracket_{\nabla}$  solves  $\llbracket P \rrbracket$ . With this example we see that the first condition in the implication is necessary.

Now, consider the nominal unification problem  $P_2 = \{a.b.(a\ b)X \approx^? b.b.(a\ b)X\}$ , and its translation as

$$\llbracket P_2 \rrbracket = \{\lambda a. \lambda b. \lambda a. \lambda b. X(b, a) = \lambda a. \lambda b. \lambda b. \lambda b. X(b, a)\}$$

In this case, the pattern substitution  $\sigma_1$  is a most general pattern unifier of  $\llbracket P_2 \rrbracket$ , and  $\sigma_2$  is a pattern unifier, but not a most general one.

Therefore, we have to require  $\text{Vars}(P) \supseteq \text{Dom}(\sigma)$ , if we want to ensure that the translation not only preserves unifiability, but also most generality.

Notice that w.l.o.g. we can require most general nominal solutions to satisfy  $\text{Vars}(P) = \text{Dom}(\sigma)$ , because most general solutions do not instantiate variables not belonging to  $\text{Vars}(P)$ , and we can always add pairs  $X \mapsto X$  for all variables occurring in  $P$  and not in  $\text{Dom}(\sigma)$ .

Notice also that in  $\sigma_2$  there are two free variables with the same name  $Y$ , but distinct types. Be aware that in  $Y \mapsto \lambda a. \lambda b. Y(b)$  the replaced  $Y$  has two arguments, whereas the introduced  $Y$  has only one argument (they have distinct types). In  $\lambda$ -calculus this is not a problem. The reason of this duplicity is that the translation function is parametric on a freshness environment  $\nabla$ . This is relevant in the case of a nominal variable. For instance,  $\llbracket Y \rrbracket_{\emptyset} = Y(a, b)$  where we use the replaced  $Y$  with two parameters, and  $\llbracket Y \rrbracket_{\{a \# Y\}} = Y(b)$  where we use the introduced  $Y$  with one parameter. If we would like to avoid this duplicity we have to forbid the use of a variable of the problem in the right-hand side of a nominal solution. Then, in our example  $P_1$ , the most general nominal solution could be written as  $\langle \{a \# Y'\}, [X \mapsto (a\ b)Y', Y \mapsto Y'] \rangle$ .

To prove that the translation of the solution of a problem is a solution of the translation of the problem, we start by proving the following two technical lemmas.

LEMMA 5.10. For any freshness environment  $\nabla$ , nominal terms  $t, u$ , and atom  $a$ , we have

- (1)  $\nabla \vdash a \# t$  if, and only if,  $a \notin \text{FV}(\llbracket t \rrbracket_{\nabla})$ , and
- (2)  $\nabla \vdash t \approx u$  if, and only if,  $\llbracket t \rrbracket_{\nabla} =_{\alpha} \llbracket u \rrbracket_{\nabla}$ .

PROOF. The first statement can be proved by routine induction on  $t$  and its translation. Notice that atoms are translated *nominally* into variables and that the binding structure is also identically translated, hence, the freshness of an atom  $a$  corresponds to the free occurrence of its variable counterpart  $a$ . We here only

comment the case  $t = \pi \cdot X$ , in this case,  $\llbracket \pi \cdot X \rrbracket_{\nabla} = X(\llbracket \pi \cdot b_1 \rrbracket_{\nabla}, \dots, \llbracket \pi \cdot b_m \rrbracket_{\nabla})$ , where  $b_i \# X \notin \nabla$ , for any  $i \in \{1..m\}$ . Therefore, we can establish the following sequence of equivalences  $\nabla \vdash a \# \pi \cdot X$  iff  $\pi^{-1} \cdot a \# X \in \nabla$  iff  $\pi^{-1} \cdot a \notin \{b_1, \dots, b_m\}$  iff  $a \notin \{\pi \cdot b_1, \dots, \pi \cdot b_m\}$  iff  $a \notin \text{FV}(X(\llbracket \pi \cdot b_1 \rrbracket_{\nabla}, \dots, \llbracket \pi \cdot b_m \rrbracket_{\nabla}))$  iff  $a \notin \text{FV}(\llbracket \pi \cdot X \rrbracket_{\nabla})$ .

The proof of the second statement can be done by induction on the equivalence  $t \approx u$ . We only comment the equivalence between suspensions:  $\pi \cdot X \approx \pi' \cdot X$ . Notice that,  $\pi \cdot X \approx \pi' \cdot X$  if, and only if, for all atoms  $a$  such that  $\pi \cdot a \neq \pi' \cdot a$ , we have  $a \# X \in \nabla$ . This condition is equivalent to: the bound variables  $\llbracket \pi \cdot a \rrbracket_{\nabla}$  and  $\llbracket \pi' \cdot a \rrbracket_{\nabla}$  are passed as a parameter to  $X$  in  $\llbracket \pi \cdot X \rrbracket_{\nabla}$  and  $\llbracket \pi' \cdot X \rrbracket_{\nabla}$  only when  $\pi \cdot a = \pi' \cdot a$ . Finally, this condition is equivalent to  $\llbracket \pi \cdot X \rrbracket_{\nabla} = \llbracket \pi' \cdot X \rrbracket_{\nabla}$ .  $\square$

The first statement of the previous lemma will not be necessary for our purposes because we have removed freshness equations.

LEMMA 5.11. *For any freshness environment  $\nabla$ , nominal substitution  $\sigma$ , and nominal term  $t$  satisfying  $\text{Vars}(t) \subseteq \text{Dom}(\sigma)$ , we have  $\llbracket \sigma \rrbracket_{\nabla}(\llbracket t \rrbracket_{\emptyset}) = \llbracket \sigma(t) \rrbracket_{\nabla}$ .*

PROOF. Again this lemma can be proved by structural induction on  $t$ . We only sketch the suspension case. Let  $t = \pi \cdot X$ . We have the equalities:

$$\begin{aligned} \llbracket \sigma \rrbracket_{\nabla}(\llbracket \pi \cdot X \rrbracket_{\emptyset}) &= [\dots, X \mapsto \lambda a_1 \dots \lambda a_n. \llbracket \sigma(X) \rrbracket_{\nabla}, \dots] (X(\llbracket \pi \cdot a_1 \rrbracket_{\nabla}, \dots, \llbracket \pi \cdot a_n \rrbracket_{\nabla})) \\ &= (\lambda a_1 \dots \lambda a_n. \llbracket \sigma(X) \rrbracket_{\nabla}) (\llbracket \pi \cdot a_1 \rrbracket_{\nabla}, \dots, \llbracket \pi \cdot a_n \rrbracket_{\nabla}) \\ &= [a_1 \mapsto \llbracket \pi \cdot a_1 \rrbracket_{\nabla}, \dots, a_n \mapsto \llbracket \pi \cdot a_n \rrbracket_{\nabla}] (\llbracket \sigma(X) \rrbracket_{\nabla}) \\ &= \llbracket \pi \cdot \sigma(X) \rrbracket_{\nabla} \\ &= \llbracket \sigma(\pi \cdot X) \rrbracket_{\nabla} \end{aligned}$$

Notice that in the first equality we use  $X \in \text{Vars}(t) \subseteq \text{Dom}(\sigma)$ , hence  $X \in \text{Dom}(\llbracket \sigma \rrbracket_{\nabla})$ .  $\square$

EXAMPLE 5.12. Let be  $t = f((a \ b) \cdot X, (a \ b) \cdot Y)$ ,  $\nabla = \{b \# Y\}$  and  $\sigma = [X \mapsto b.a, Y \mapsto Y]$ . We will have

$$\begin{aligned} \llbracket \sigma \rrbracket_{\nabla} &= \llbracket [X \mapsto b.a, Y \mapsto Y] \rrbracket_{\{b \# Y\}} = [X \mapsto \lambda a. \lambda b. \llbracket b.a \rrbracket_{\{b \# Y\}}, Y \mapsto \lambda a. \lambda b. \llbracket Y \rrbracket_{\{b \# Y\}}] \\ &= [X \mapsto \lambda a. \lambda b. \lambda b.a, Y \mapsto \lambda a. \lambda b. Y(a)] \\ \llbracket t \rrbracket_{\emptyset} &= \llbracket f((a \ b) \cdot X, (a \ b) \cdot Y) \rrbracket_{\emptyset} = f(X(b, a), Y(b, a)) \\ \llbracket \sigma(t) \rrbracket_{\nabla} &= \llbracket [X \mapsto b.a, Y \mapsto Y] f((a \ b) \cdot X, (a \ b) \cdot Y) \rrbracket_{\{b \# Y\}} = \llbracket f(a.b, (a \ b) \cdot Y) \rrbracket_{\{b \# Y\}} \\ &= f(\lambda a. b, Y(b)) \end{aligned}$$

Now, we have

$$\begin{aligned} \llbracket \sigma \rrbracket_{\nabla}(\llbracket t \rrbracket_{\emptyset}) &= f(\underline{(\lambda a. \lambda b. \lambda b.a)(b, a)}, (\lambda a. \lambda b. Y(a))(b, a)) = f(\lambda c. b, Y(b)) = f(\lambda a. b, Y(b)) \\ &= \llbracket \sigma(t) \rrbracket_{\nabla} \end{aligned}$$

Notice that the substitution resulting from the  $\beta$ -reduction of the underlined redex needs to avoid a capture of  $b$ . This is done replacing the bound variable  $b$  by  $c$ . In the following section we will see that, in pattern unification, we can do this without using new bound variable names. In this case, we could have used  $a$  instead of  $c$ .

From these two lemmas we can prove the following results.

**THEOREM 5.13.** *For any freshness environment  $\nabla$ , equational nominal unification problem  $P$ , and nominal substitution  $\sigma$  with  $\text{Vars}(P) \subseteq \text{Dom}(\sigma)$ , we have that  $\langle \nabla, \sigma \rangle$  solves the equational nominal unification problem  $P$ , if, and only if,  $\llbracket \sigma \rrbracket_{\nabla}$  solves the pattern unification problem  $\llbracket P \rrbracket$ .*

**PROOF.** By definition of nominal solution, the pair  $\langle \nabla, \sigma \rangle$  solves  $P$  iff

$$\nabla \vdash \sigma(t) \approx \sigma(u) \quad \text{for all } t \approx^? u \in P$$

By Lemma 5.10 this is equivalent to:

$$\llbracket \sigma(t) \rrbracket_{\nabla} =_{\alpha} \llbracket \sigma(u) \rrbracket_{\nabla} \quad \text{for all } t \approx^? u \in P$$

and, by Lemma 5.11 this is equivalent to:

$$\llbracket \sigma \rrbracket_{\nabla}(\llbracket t \rrbracket_{\emptyset}) = \llbracket \sigma \rrbracket_{\nabla}(\llbracket u \rrbracket_{\emptyset}) \quad \text{for all } t \approx^? u \in P$$

Since the substitution  $\llbracket \sigma \rrbracket_{\nabla}$  does not instantiate the variables  $a_1, \dots, a_n$ , this is equivalent to (see Remark 5.14):

$$\llbracket \sigma \rrbracket_{\nabla}(\lambda a_1 \dots \lambda a_n. \llbracket t \rrbracket_{\emptyset}) = \llbracket \sigma \rrbracket_{\nabla}(\lambda a_1 \dots \lambda a_n. \llbracket u \rrbracket_{\emptyset}) \quad \text{for all } t \approx^? u \in P$$

where  $\langle a_1, \dots, a_n \rangle$  is the list of atoms occurring in  $P$ .

Finally, since  $\llbracket t \approx^? u \rrbracket = \lambda a_1 \dots \lambda a_n. \llbracket t \rrbracket_{\emptyset} \stackrel{?}{=} \lambda a_1 \dots \lambda a_n. \llbracket u \rrbracket_{\emptyset}$ , this is equivalent to  $\llbracket \sigma \rrbracket_{\nabla}$  solves  $\llbracket P \rrbracket$ .  $\square$

The proof of Theorem 5.13 also allows us to prove that  $\langle \nabla, \sigma \rangle$  solves  $t \approx^? u$ , if, and only if,  $\llbracket \sigma \rrbracket_{\nabla}$  solves  $\llbracket t \rrbracket_{\emptyset} \stackrel{?}{=} \llbracket u \rrbracket_{\emptyset}$ . Therefore, it seems unnecessary to add the  $\lambda$ -bindings  $\lambda a_1 \dots \lambda a_n$  in front of both sides of the higher-order equations, as was suggested in Example 3.4. The following remark illustrates what would happen if we had defined translation of equations in this way.

**REMARK 5.14.** *Assume that we had defined  $\llbracket t \approx^? u \rrbracket = \llbracket t \rrbracket_{\emptyset} \stackrel{?}{=} \llbracket u \rrbracket_{\emptyset}$ , instead of the definition we have for  $\llbracket t \approx^? u \rrbracket$  with the external lambda's.*

*The translation of the unsolvable nominal equation  $a \approx^? b$  would result into  $a \stackrel{?}{=} b$  which is solvable by  $[a \mapsto b]$  (notice that, in this case, atoms are translated into free variables). The example does not contradict Theorem 5.13 because the substitution  $[a \mapsto b]$  is not the translation of any nominal substitution, i.e. there does not exist a freshness environment  $\nabla$  and a nominal substitution  $\sigma$  such that  $\llbracket \sigma \rrbracket_{\nabla} = [a \mapsto b]$ . If we introduce the external  $\lambda$ -bindings we get the unsolvable higher-order unification problem  $\lambda a. \lambda b. a \stackrel{?}{=} \lambda a. \lambda b. b$ .*

*On the other hand, the translation of the solvable nominal equation of Example 3.4 would be*

$$\llbracket P \rrbracket = \llbracket \{a.b.f(b, X_6) \approx^? a.a.f(a, X_7)\} \rrbracket = \{\lambda a. \lambda b. f(b, X_6(a, b)) \stackrel{?}{=} \lambda a. \lambda a. f(a, X_7(a, b))\}$$

*that is not a higher-order pattern unification problem (notice that Lemma 5.7 does not hold if we do not introduce the external  $\lambda$ -bindings).*

*The translation of its nominal most general solution is*

$$\llbracket \sigma \rrbracket_{\nabla} = \llbracket [X_6 \mapsto (b \ a) \cdot X_7] \rrbracket_{\{b \# x_7\}} = [X_6 \mapsto \lambda a. \lambda b. X_7(b), X_7 \mapsto \lambda a. \lambda b. X_7(a)]$$



In this case,  $\llbracket \sigma \rrbracket_{\nabla}$  is a higher-order unifier of  $\llbracket P \rrbracket$ , as Theorem 5.13 predicts. However, it is not a most general unifier, and we are interested in translating most general solutions into most general solutions.

**THEOREM 5.15.** *If the equational nominal unification problem  $P$  is solvable, then the higher-order pattern unification problem  $\llbracket P \rrbracket$  is also solvable.*

**PROOF.** The theorem is a direct consequence of Theorem 5.13.  $\square$

The opposite implication of Theorem 5.15 can not be directly proved from Theorem 5.13, because  $\llbracket P \rrbracket$  should have solutions that are not of the form  $\llbracket \sigma \rrbracket_{\nabla}$ , for any solution  $\langle \nabla, \sigma \rangle$  of  $P$ .

## 6. SOME PROPERTIES OF PATTERN UNIFICATION

In this section we prove some fundamental properties of Higher-Order Pattern Unification. In particular, we prove that we can express most general unifiers of pattern unification problems only using bound-variable names and types already used in the problem. This property is used in next sections in the translation of pattern unifiers into nominal unifiers.

In the following example we note that in the solution of pattern unification problems it is important to *save names* of bound variables. In the following we will distinguish between variables and variable names. For instance  $\lambda x.\lambda x.x$  has three occurrences of variables, two distinct variables, with one unique variable name. Notice that  $\alpha$ -conversion preserves the number of variables, but may change the number of names.

**EXAMPLE 6.1.** Consider the nominal problem  $a.X \stackrel{?}{\approx} a.f(b.Y)$ . Its translation is  $\lambda a.\lambda b.\lambda a.X(a, b) \stackrel{?}{=} \lambda a.\lambda b.\lambda a.f(\lambda b.Y(a, b))$ . An  $\alpha$ -conversion results in  $\lambda a.\lambda b.\lambda c.X(c, b) \stackrel{?}{=} \lambda a.\lambda b.\lambda c.f(\lambda d.Y(c, d))$  and it shows that the parameters of  $X$  and  $Y$  are in fact different. A most general solution is  $[X \mapsto \lambda c.\lambda b.f(\lambda d.Y(c, d))]$ . Since  $Y$  is translated as  $Y(a, b)$ , we would have to translate back  $Y(c, d)$  as  $(a\ c)(d\ b) \cdot Y$ . And, since substitutions like  $[X \mapsto t]$  are translated as  $[X \mapsto \lambda a.\lambda b.\llbracket t \rrbracket_{\nabla}]$ , we would have to translate back  $[X \mapsto \lambda c.\lambda b.\llbracket t \rrbracket_{\nabla}]$  as  $[X \mapsto (a\ c) \cdot t]$ . Therefore, our pattern unifier had to be translated back as  $[X \mapsto (a\ c) \cdot f(d.(a\ c)(d\ b) \cdot Y)]$ . However, the list of atoms is fixed as the list of atoms occurring in the problem, hence, we know how to translate  $a$  and  $b$  as  $a$  and  $b$  and vice versa, but we do not know how to translate back  $c$  and  $d$ . Here it is done introducing new atoms. However, the use of an infinite list of atom names would imply that the list of arguments of a variable (the list of capturable atoms) would be infinite.

If we look at Nipkow's transformation rules described in Subsection 2.2, it seems that no new bound-variable names are introduced. However, this is not true. There are three places where their introduction is hidden. In the following we illustrate these cases.

- (1) It is assumed that equations have the same most external  $\lambda$ -bindings, i.e. that they are of the form  $\lambda \vec{x}.s \stackrel{?}{=} \lambda \vec{x}.t$ . If this is not the case, we have to  $\alpha$ -convert one of the sides. However, this is not always possible without introducing new bound-variable names. For instance, if we have the equation  $\lambda x.\lambda y.\lambda y.X(x, y) \stackrel{?}{=} \lambda y.\lambda y.\lambda x.Y(x, y)$ , after  $\alpha$ -converting the two most

external  $\lambda$ -binder, we get  $\lambda x.\lambda y.\lambda y.X(x, y) \stackrel{?}{=} \lambda x.\lambda y.\lambda x.Y(x, y)$ , that needs a new bound-variable name to obtain the same  $\lambda$ -binders in both sides, by means of  $\alpha$ -conversion. Using a *new name*  $z$  we would get  $\lambda x.\lambda y.\lambda z.X(x, z) \stackrel{?}{=} \lambda x.\lambda y.\lambda z.Y(z, y)$ .

- (2) In the flex-rigid rule the terms  $u_i$  may not be of first-order type. In this case, we need to  $\eta$ -expand some subterms. For instance, the rule transforms  $\lambda x.X(x) \stackrel{?}{=} \lambda x.f(\lambda x.g(x))$  into the equation  $\lambda x.X_1(x) \stackrel{?}{=} \lambda x.\lambda x.g(x)$  and the substitution  $[X \mapsto \lambda x.f(X_1(x))]$ . The left-hand side of the equation needs to be  $\eta$ -expanded, and we can not use the name  $x$ . Using a *new name*  $z$ , and  $\alpha$ -converting we would get  $\lambda x.\lambda z.X_1(x, z) \stackrel{?}{=} \lambda x.\lambda z.g(z)$ .
- (3) When we compute a substitution for a variable, it must be applied to all the occurrences of the variable, and this may involve a  $\beta$ -reduction. Some  $\beta$ -reductions need to introduce new names to avoid variable-captures. For instance, if we have the equations  $\{\lambda x.\lambda y.X(x, y) \stackrel{?}{=} \lambda x.\lambda y.f(\lambda x.Y(x, y)), \lambda x.\lambda y.Z(x, y) \stackrel{?}{=} \lambda x.\lambda y.X(y, x)\}$ , after solving the first one we get  $[X \mapsto \lambda x.\lambda y.f(\lambda x.Y(x, y))]$  that must be substituted in the second equation. We get,  $\lambda x.\lambda y.Z(x, y) \stackrel{?}{=} \lambda x.\lambda y.(\lambda x.\lambda y.f(\lambda x.Y(x, y)))(y, x)$ . The  $\beta$ -reduction using the standard substitution algorithm introduces a *new name*  $z$  to avoid the capture of the variable  $x$ , giving  $\lambda x.\lambda y.Z(x, y) \stackrel{?}{=} \lambda x.\lambda y.f(\lambda z.Y(z, x))$

In the following we show how we can overcome these problems. One of the ideas is using a kind of swapping for  $\lambda$ -calculus, instead of the usual substitution, like it is done in nominal terms.

**DEFINITION 6.2.** *Given two variables  $x, y$ , and a  $\lambda$ -term  $t$ , we define the swapping of  $x$  and  $y$  in  $t$ , noted by  $(xy) \cdot t$  inductively as follows*

$$\begin{aligned}
 (xy) \cdot x &= y \\
 (xy) \cdot y &= x \\
 (xy) \cdot z &= z && \text{if } z \neq x, y \\
 (xy) \cdot c &= c \\
 (xy) \cdot (\lambda z.t) &= \lambda((xy) \cdot z).((xy) \cdot t) \\
 (xy) \cdot (a(t_1, \dots, t_n)) &= ((xy) \cdot a)((xy) \cdot t_1, \dots, (xy) \cdot t_n)
 \end{aligned}$$

where  $c$  is a constant and  $a$  is a constant or a variable.

Notice that this swapping is distinct from the swapping on nominal terms. In particular  $(ab)X = X$ , and we do not keep suspensions. In some cases its application results into an  $\alpha$ -equivalent term, but in general the result is a different term.

**REMARK 6.3.** *In  $\lambda$ -calculus, following the Barendregt variable convention, operations are defined on classes of  $\alpha$ -equivalent terms, rather than on particular terms. This, for instance, allows us to freely  $\alpha$ -convert terms in substitutions in order to avoid variable capture. Therefore, (although it is often omitted) we have to prove that the operation is independent of the representative of the class that we take. The previous swapping operation is defined for particular terms. However, the following lemma ensures that it can be extended to  $\alpha$ -equivalent classes of terms. Barendregt variable convention suggests to use distinct variable names for distinct variables.*

Here, since we try to avoid the introduction of new variable names, we do not use the convention, and work with particular terms.

LEMMA 6.4. For any term  $t$  and variables  $x$  and  $y$ , we have

$$(x y) \cdot t =_{\alpha} [x \mapsto y, y \mapsto x] t$$

where  $[x \mapsto y, y \mapsto x]$  changes  $x$  by  $y$  and  $y$  by  $x$  in  $t$ , simultaneously.

In particular, if  $x, y \notin \text{FV}(t)$ , then  $(x y) \cdot t =_{\alpha} t$ .

PROOF. By structural induction on  $t$ . For one of the cases of  $\lambda$ -abstraction, for instance, we have

$$\begin{aligned} (x y) \lambda x. t &= \lambda y. (x y) t && \text{By induct. hypothesis} \\ &= \lambda y. [x \mapsto y, y \mapsto x] t && \text{Let be } z \notin \text{FV}(t) \cup \{x, y\} \\ &= \lambda y. [z \mapsto y][y \mapsto x][x \mapsto z] t && \text{Since } y \notin \text{FV}([y \mapsto x][x \mapsto z] t) \\ &=_{\alpha} \lambda z. [y \mapsto x][x \mapsto z] t && \text{Since } z \neq x, y \\ &= [y \mapsto x] \lambda z. [x \mapsto z] t && \text{Since } z \notin \text{FV}(t) \\ &=_{\alpha} [y \mapsto x] \lambda x. t && \text{Since } x \notin \text{FV}(\lambda x. t) \\ &= [x \mapsto y, y \mapsto x] \lambda x. t \end{aligned}$$

□

LEMMA 6.5. If  $\vec{y}$  is a list of pairwise distinct variable names<sup>5</sup>,  $|\vec{y}| = |\vec{x}| = n$  and  $\{\vec{y}\} \cap \text{FV}(\lambda \vec{x}. t) = \emptyset$ , then

$$(\lambda \vec{x}. t)(\vec{y}) = \Pi_n(\vec{x}, \vec{y}) \cdot t$$

where  $\Pi_n(\vec{x}, \vec{y})$  is a permutation on the names  $\vec{x}, \vec{y}$  defined inductively as

$$\begin{aligned} \Pi_1(\langle x \rangle, \langle y \rangle) &= (x y) \\ \Pi_n(\langle x_1, \dots, x_n \rangle, \langle y_1, \dots, y_n \rangle) &= \Pi_{n-1}(\langle (x_1 y_1) \cdot x_2, \dots, (x_1 y_1) \cdot x_n \rangle, \langle y_2, \dots, y_n \rangle) \cdot (x_1 y_1) \end{aligned}$$

PROOF. By induction on the length  $n$  of both vectors. Obviously, the variable  $x_1$  is not free in  $\lambda x_1. \lambda x_2, \dots, x_n. t$ . By assumption, the variable  $y_1$  is neither free in this term.

From  $\text{FV}(\lambda x_2, \dots, x_n. t) \subseteq \text{FV}(\lambda \vec{x}. t) \cup \{x_1\}$ , and  $x_1, y_1 \notin \text{FV}(\lambda \vec{x}. t)$ , we have  $\text{FV}((x_1 y_1) \cdot (\lambda x_2, \dots, x_n. t)) \subseteq \text{FV}(\lambda \vec{x}. t) \cup \{y_1\}$ . Since  $y_1 \notin \{y_2, \dots, y_n\}$  and  $\{\vec{y}\} \cap \text{FV}(\lambda \vec{x}. t) = \emptyset$ , we have  $\{y_2, \dots, y_n\} \cap \text{FV}((x_1 y_1) \cdot (\lambda x_2, \dots, x_n. t)) = \emptyset$ . Therefore, we can apply the induction hypothesis to the term  $(x_1 y_1) \cdot (\lambda x_2, \dots, x_n. t)$  and the vector  $(y_2, \dots, y_n)$ , obtaining

$$\begin{aligned} (\lambda \vec{x}. t)(\vec{y}) &=_{\alpha} (\lambda y_1. (x_1 y_1) \cdot (\lambda x_2, \dots, x_n. t))(y_1, y_2, \dots, y_n) && \text{By Lemma 6.4} \\ &=_{\beta} ((x_1 y_1) \cdot (\lambda x_2, \dots, x_n. t))(y_2, \dots, y_n) && \text{By } \beta\text{-reduction} \\ &= (\lambda (x_1 y_1) \cdot x_2, \dots, (x_1 y_1) \cdot x_n. (x_1 y_1) \cdot t)(y_2, \dots, y_n) && \text{By def. of swapping} \\ &= \Pi_{n-1}(\langle (x_1 y_1) \cdot x_2, \dots, (x_1 y_1) \cdot x_n \rangle, \langle y_2, \dots, y_n \rangle) \cdot (x_1 y_1) \cdot t && \text{By induct. hypothesis} \\ &= \Pi_n(\vec{x}, \vec{y}) \cdot t \end{aligned}$$

□

<sup>5</sup>Notice that we do not require  $\vec{x}$  to be pairwise distinct. If they are also pairwise distinct, then  $\Pi_n(\vec{x}, \vec{y}) = (x_n y_n) \dots (x_1 y_1)$ .

Now we will describe a variant of the higher-order pattern unification algorithm of Section 2.2. In this variant, external  $\lambda$ -binders are  $\alpha$ -converted explicitly and the flex-rigid rule has been replaced by a new rule where  $\eta$ -expansion is made explicit, i.e. the terms  $u_i$  are base-typed, thus the right-hand side does not need to be  $\eta$ -expanded, like in the original rule. Moreover,  $\beta$ -redexes are removed using swappings, according to Lemma 6.5, since we are dealing with patterns.

**DEFINITION 6.6.** *We assume unoriented equations and define the following set of transformation rules over higher-order pattern equations:*

**$\alpha$ -transformation:**

$$\begin{aligned} \lambda\vec{w}. \lambda x. t &\stackrel{?}{=} \lambda\vec{w}. \lambda y. u \rightarrow \langle \lambda\vec{w}. \lambda x. t \stackrel{?}{=} \lambda\vec{w}. (x \ y) \cdot (\lambda y. u), [ ] \rangle \\ &\quad \text{if } x \notin \text{FV}(u) \\ \lambda\vec{w}. \lambda x. t &\stackrel{?}{=} \lambda\vec{w}. \lambda x. u \rightarrow \langle \lambda\vec{w}. t \stackrel{?}{=} \lambda\vec{w}. u, [ ] \rangle \\ &\quad \text{if } x \notin \text{FV}(t) \text{ and } x \notin \text{FV}(u) \\ \lambda\vec{w}. \lambda x. t &\stackrel{?}{=} \lambda\vec{w}. \lambda x. u \rightarrow \langle \lambda\vec{w}. \lambda x. t \stackrel{?}{=} \lambda\vec{w}. \lambda x. u, [X \mapsto \lambda\vec{y}. Z(\vec{z})] \rangle \\ &\quad \text{if } x \notin \text{FV}(t), X(\vec{y}) \text{ is a subterm of } u, \\ &\quad \text{ } x \in \{\vec{y}\} \text{ and } \{\vec{z}\} = \{\vec{y}\} \setminus \{x\} \end{aligned}$$

**Rigid-rigid:**

$$\lambda\vec{w}. a(t_1, \dots, t_n) \stackrel{?}{=} \lambda\vec{w}. a(u_1, \dots, u_n) \rightarrow \langle \{\lambda\vec{w}. t_1 \stackrel{?}{=} \lambda\vec{w}. u_1, \dots, \lambda\vec{w}. t_n \stackrel{?}{=} \lambda\vec{w}. u_n\}, [ ] \rangle$$

**Flex-rigid:**

$$\begin{aligned} \lambda\vec{w}. X(\vec{x}) &\stackrel{?}{=} \lambda\vec{w}. a(\lambda\vec{y}_1. u_1, \dots, \lambda\vec{y}_m. u_m) \rightarrow \left\langle \left\{ \begin{array}{l} \lambda\vec{w}. \lambda\vec{y}_1. X_1(\vec{z}_1) \stackrel{?}{=} \lambda\vec{w}. \lambda\vec{y}_1. u_1, \\ \dots \\ \lambda\vec{w}. \lambda\vec{y}_m. X_m(\vec{z}_m) \stackrel{?}{=} \lambda\vec{w}. \lambda\vec{y}_m. u_m, \end{array} \right. \right. \\ &\quad \left. \left. [X \mapsto \lambda\vec{x}. a(\lambda\vec{y}_1. X_1(\vec{z}_1), \dots, \lambda\vec{y}_m. X_m(\vec{z}_m))] \right\rangle \right. \\ &\quad \text{if } X \notin \text{FV}(u_i), a \text{ is a constant or } a \in \{\vec{x}\}, \\ &\quad \text{and } \{\vec{z}_i\} = \{\vec{x}\} \cup \{\vec{y}_i\}, \text{ for } i = 1, \dots, m. \end{aligned}$$

**Flex-flex:**

$$\begin{aligned} \lambda\vec{w}. X(\vec{x}) &\stackrel{?}{=} \lambda\vec{w}. X(\vec{y}) \rightarrow \langle \emptyset, [X \mapsto \lambda\vec{x}. Z(\vec{z})] \rangle \\ &\quad \text{where } \{\vec{z}\} = \{x_i \mid x_i = y_i\} \\ \lambda\vec{w}. X(\vec{x}) &\stackrel{?}{=} \lambda\vec{w}. Y(\vec{y}) \rightarrow \langle \emptyset, [X \mapsto \lambda\vec{x}. Z(\vec{z}), Y \mapsto \lambda\vec{y}. Z(\vec{z})] \rangle \\ &\quad \text{where } X \neq Y \text{ and } \{\vec{z}\} = \{\vec{x}\} \cap \{\vec{y}\} \end{aligned}$$

*These transformations are applied as follows. The equation on the left-hand side is replaced by the equations in the first component of the right-hand side, and then the substitution in the second component of the right-hand side is applied to all the equations. If this substitution introduces  $\beta$ -redexes, they are removed using swappings, according to Lemma 6.5. Moreover, all the substitutions are composed to compute the resulting unifier. In other words, the transformation is applied as follows  $\langle \{e\} \cup E, \sigma \rangle \rightarrow \langle \sigma'(E' \cup E) \downarrow_{\beta}, \sigma' \circ \sigma \rangle$ , if we have a transformation  $e \rightarrow \langle E', \sigma' \rangle$ .*

With the following examples, we illustrate how these rules solve the problems concerning the introduction of new bound variable names described previously, at

the beginning of this section.

EXAMPLE 6.7. Given the equation  $\lambda x.\lambda y.\lambda y.X(x, y) \stackrel{?}{=} \lambda y.\lambda y.\lambda x.Y(x, y)$  the application of the first  $\alpha$ -transformation rule gives us  $\lambda x.\lambda y.\lambda y.X(x, y) \stackrel{?}{=} \lambda x.\lambda x.\lambda y.Y(y, x)$ . A second application of this  $\alpha$ -transformation gives us  $\lambda x.\lambda y.\lambda y.X(x, y) \stackrel{?}{=} \lambda x.\lambda y.\lambda x.Y(x, y)$ . Now, the first  $\alpha$ -transformation rule is no longer applicable. However, we can apply the third  $\alpha$ -transformation rule, that instantiates  $[X \mapsto \lambda x.\lambda y.X'(y)]$ , and gives the equation  $\lambda x.\lambda y.\lambda y.X'(y) \stackrel{?}{=} \lambda x.\lambda y.\lambda x.Y(x, y)$ . Now, applying the second  $\alpha$ -transformation rule, we obtain  $\lambda y.\lambda y.X'(y) \stackrel{?}{=} \lambda y.\lambda x.Y(x, y)$ . Again, we can apply the third  $\alpha$ -transformation rule, that instantiates  $[Y \mapsto \lambda x.\lambda y.Y'(x)]$ , and gives  $\lambda y.\lambda y.X'(y) \stackrel{?}{=} \lambda y.\lambda x.Y'(x)$ . The first  $\alpha$ -transformation rule gives  $\lambda y.\lambda y.X'(y) \stackrel{?}{=} \lambda y.\lambda y.Y'(y)$ . Finally, the second  $\alpha$ -transformation rule gives  $\lambda y.X'(y) \stackrel{?}{=} \lambda y.Y'(y)$ .

This last equation can be solved applying the second flex-flex rule. The resulting unifier is

$$\begin{aligned} & [X' \mapsto \lambda y.Z(y), Y' \mapsto \lambda y.Z(y)] \circ [Y \mapsto \lambda x.\lambda y.Y'(x)] \circ [X \mapsto \lambda x.\lambda y.X'(y)] \Big|_{\{X, Y\}} \\ &= [X \mapsto \lambda x.\lambda y.Z(y), Y \mapsto \lambda x.\lambda y.Z(x)] \end{aligned}$$

EXAMPLE 6.8. The new flex-rigid rule transforms  $\lambda x.X(x) \stackrel{?}{=} \lambda x.f(\lambda y.a)$  into the equation  $\lambda x.\lambda y.X_1(x, y) \stackrel{?}{=} \lambda x.\lambda y.a$  and the substitution  $[X \mapsto \lambda x.f(\lambda y.X_1(x, y))]$ . The original flex-rigid rule would give us  $\lambda x.X_1(x) \stackrel{?}{=} \lambda x.\lambda y.a$ , that conveniently  $\eta$ -expanded using the same variable name  $y$ , results into the same equation. A further application of the flex-rigid rule solves the equation by  $[X_1 \mapsto \lambda x.\lambda y.a]$ .

In other cases, the resulting equation may be different. The new rule transforms  $\lambda x.X(x) \stackrel{?}{=} \lambda x.f(\lambda x.g(x))$  into the equation  $\lambda x.\lambda x.X_1(x) \stackrel{?}{=} \lambda x.\lambda x.g(x)$  and the substitution  $[X \mapsto \lambda x.f(\lambda x.X_1(x))]$ . However, the original flex-rigid rule would give us  $\lambda x.X_1(x) \stackrel{?}{=} \lambda x.\lambda x.g(x)$  and the substitution  $[X \mapsto \lambda x.f(X_1(x))]$ . In the subsequent  $\eta$ -expansion we can not use the name  $x$ , and we need a *new name*  $z$ , and  $\alpha$ -conversion of the right-hand side getting  $\lambda x.\lambda z.X_1(x, z) \stackrel{?}{=} \lambda x.\lambda z.g(z)$ . Both equations are obviously distinct. However, to solve this second equation,  $X_1$  can not use the first argument, because it is not used in the right-hand side. Therefore, we can instantiate  $X_1 \mapsto \lambda x.\lambda y.X'_1(y)$ , and  $\alpha$ -convert the new variable name  $z$ , getting the same equation as with the new flex-rigid rule.

EXAMPLE 6.9. Given the equations  $\{\lambda x.\lambda y.X(x, y) \stackrel{?}{=} \lambda x.\lambda y.f(\lambda x.Y(x, y)), \lambda x.\lambda y.Z(x, y) \stackrel{?}{=} \lambda x.\lambda y.X(y, x)\}$ , after solving the first equation and replacing  $[X \mapsto \lambda x.\lambda y.f(\lambda x.Y(x, y))]$  into the second one, we get  $\lambda x.\lambda y.Z(x, y) \stackrel{?}{=} \lambda x.\lambda y.((\lambda x.\lambda y.f(\lambda x.Y(x, y)))(y, x))$ . By Lemma 6.5, we can  $\beta$ -reduce using swapings, instead of the usual standard substitution. The permutation will be  $\Pi_2(\langle x, y \rangle, \langle y, x \rangle) = \Pi_1(\langle (xy) \cdot y, \langle x \rangle \rangle \cdot (xy) = (xx) \cdot (xy) = (xy)$ , and the result of the  $\beta$ -reduction will be

$$(\lambda x.\lambda y.f(\lambda x.Y(x, y)))(y, x) =_{\beta} (xy) \cdot f(\lambda x.Y(x, y)) = f(\lambda y.Y(y, x))$$

LEMMA 6.10. *The algorithm described in Definition 6.6 is sound and complete and computes a most-general higher-order pattern unifier whenever it exists, when names of free and bound variables are disjoint.*

PROOF. The algorithm computes basically the same most general unifiers than the Nipkow's algorithm.

The fact that we use swapping instead of substitution to remove  $\beta$ -redexes is not a problem according to Lemma 6.5. We will obtain a term that is  $\alpha$ -equivalent to the one that we would obtain with the traditional capture-avoiding substitution. Notice that in the lemma we require arguments of free variables (the sequence  $\vec{y}$ ) to be a list of distinct bound variables. This is ensured in the case of higher-order pattern unification, but it is not true in the general  $\lambda$ -calculus. The algorithm preserves the disjointness of bound and free variable names. Therefore, the other condition of the lemma  $\{\vec{y}\} \cap \text{FV}(\lambda\vec{x}.t)$  is also satisfied.

In the third  $\alpha$ -transformation rule, if  $x \notin \text{FV}(t)$  and  $x \in \text{FV}(u)$  and the equation is solvable, then  $x$  must occur in  $u$  just below a free variable, as one of its arguments, and this free variable must be instantiated by a term that does not use this argument. Notice also that the three  $\alpha$ -transformation rules, when the equation is solvable, succeed in making the lists of most external  $\lambda$ -bindings equal in both sides of the equation.

In the case of the flex-rigid rule, we may obtain an equation  $\lambda\vec{x}.X_i(x_1, \dots, x_n) \stackrel{?}{=} \lambda\vec{x}.\lambda\vec{y}.u'_i$  that needs to be  $\eta$ -expanded, and where  $\{x_1, \dots, x_n\} \cap \{\vec{y}\} \neq \emptyset$ . Let be  $\{x'_1, \dots, x'_{n'}\} = \{x_1, \dots, x_n\} \setminus \vec{y}$ , i.e. the sequence of variables  $x_i$ 's not in  $\vec{y}$ . In any solution of this equation  $X_i$  can not use the variables of the intersection of  $\{x_1, \dots, x_n\} \cap \{\vec{y}\}$ . Therefore, we can extend the solution with  $X_i \mapsto \lambda x_1, \dots, x_n.\lambda\vec{y}.X'_i(x'_1, \dots, x'_{n'}, \vec{y})$ , and get the equation  $\lambda\vec{x}.\lambda\vec{y}.X'_i(x'_1, \dots, x'_{n'}, \vec{y}) \stackrel{?}{=} \lambda\vec{x}.\lambda\vec{y}.u'_i$ .

The flex-flex and rigid-rigid rules are the same as in Nipkow's algorithm.  $\square$

LEMMA 6.11. *Let  $P$  be a solvable pattern unification problem, where the set of free and bound variable names are disjoint, and let  $\langle a_1, \dots, a_n \rangle$  be a list of the names of bound variables of the problem. Then, there exists a most general unifier  $\sigma$  such that*

- (1)  *$\sigma$  does not use other bound-variable names than the ones already used in the problem, i.e. than  $\{a_1, \dots, a_n\}$ .*

*If in the original problem all bound variables with the same name have the same type, i.e. we have a type  $\tau_i$  for every bound variable name  $a_i$ , then*

- (2) *the same applies to  $\sigma$ , i.e. any bound variable of  $\sigma$  with name  $a_i$  has type  $\tau_i$ , and*
- (3) *any free variable  $X$  occurring in  $\sigma$  has type  $\nu_1 \rightarrow \dots \rightarrow \nu_m \rightarrow \nu$ , where  $\langle \nu_1, \dots, \nu_m \rangle$  is a sublist of  $\langle \tau_1, \dots, \tau_n \rangle$ .*

PROOF. By Lemma 6.10 with the new transformation rules we obtain most general unifiers for solvable pattern unification problems. Then, by simple inspection of the new transformation rules, where all bound variable names in the right-hand sides of the rules are already present in the left-hand sides, we have that new equations and substitutions do not introduce new names. In addition, since names of free and bound variables are distinct,  $\beta$ -reductions due to substitution applications satisfy conditions of Lemma 6.5, therefore we can conclude that we do not need new bound variable names due to  $\beta$ -reductions either.

Notice also that in these rules, when we introduce a new bound variable in the right-hand side, with a name already used in the left-hand side, both variables have the same type. When, we swap two variable names in an  $\alpha$ -conversion or in a  $\beta$ -reduction, they have also the same type.

Finally, let  $\sigma'$  be any most general unifier not using other bound variable names than the ones used in  $P$ , i.e.  $a_1, \dots, a_n$ . For every variable  $X$  occurring free in  $\sigma$ , chose one of their occurrences. This will be of the form  $X(b_1, \dots, b_m)$ , where  $\{b_1, \dots, b_m\} \subseteq \{a_1, \dots, a_n\}$  and the  $b_i$ 's are pairwise distinct. Let  $\langle b_{\pi(1)}, \dots, b_{\pi(m)} \rangle$  be a sublist of  $\langle a_1, \dots, a_n \rangle$ . Then composing  $\sigma'$  with  $[X' \mapsto \lambda b_1. \dots \lambda b_m. X(b_{\pi(1)}, \dots, b_{\pi(m)})]$ , for every variable  $X$ , we get another most general unifier fulfilling the requirements of the third statement of the lemma. Notice that, although not all occurrences of  $X$  have the same parameters, it does not matter which one we chose because all them have the same type.  $\square$

## 7. THE REVERSE TRANSLATION

As we have shown, Theorem 5.13 is not enough to prove that, if  $\llbracket P \rrbracket$  is solvable, then  $P$  is solvable. We still have to prove that if  $\llbracket P \rrbracket$  is solvable, then for some solution  $\sigma$  of  $\llbracket P \rrbracket$  we can build a nominal solution  $\langle \nabla, \sigma' \rangle$  of  $P$ . This is the main objective of this section. Taking into account that  $\llbracket P \rrbracket$  is a higher-order pattern unification problem, and that these problems are unitary, we will prove something stronger: if  $\llbracket P \rrbracket$  is solvable, then  $\llbracket \sigma \rrbracket^{-1}$  is defined for the most general unifier  $\sigma$  of  $\llbracket P \rrbracket$ . Moreover, in the next section we will prove that  $\llbracket \sigma \rrbracket^{-1}$  is also a most general nominal unifier.

**DEFINITION 7.1.** *Let  $\langle a_1, \dots, a_n \rangle$  be a fixed ordered list of atoms, and let  $\nabla$  be a freshness environment. The back-translation function is defined on  $\lambda$ -terms in  $\eta$ -long  $\beta$ -normal form as follows:*

$$\begin{aligned} \llbracket a \rrbracket^{-1}_{\nabla} &= a \\ \llbracket f(t_1, \dots, t_n) \rrbracket^{-1}_{\nabla} &= f(\llbracket t_1 \rrbracket^{-1}_{\nabla}, \dots, \llbracket t_n \rrbracket^{-1}_{\nabla}) \\ \llbracket \lambda a. t \rrbracket^{-1}_{\nabla} &= a. \llbracket t \rrbracket^{-1}_{\nabla} \\ \llbracket X(c_1, \dots, c_m) \rrbracket^{-1}_{\nabla} &= \pi^{-1}.X \quad \text{where } \pi \text{ is a permutation on } \langle a_1, \dots, a_n \rangle \text{ satisfying} \\ &\quad \langle \pi \cdot c_1, \dots, \pi \cdot c_m \rangle \text{ is the sublist of } \langle a_1, \dots, a_n \rangle \text{ such that} \\ &\quad \pi \cdot c_i \# X \notin \nabla \text{ and } c_i \text{ and } \pi \cdot c_i \text{ have the same sort} \end{aligned}$$

where  $a$  is a bound variable with name  $a$ ,  $f$  is the constant associated to the function symbol  $f$ , either  $X$  is the free variable associated to  $X$ , or if  $X$  is a fresh variable then  $X$  is a fresh nominal variable, and the permutation  $\pi^{-1}$  is supposed to be decomposed in terms of transpositions (swappings).

Notice that the back-translation function is not defined for all  $\lambda$ -terms, even for all higher-order patterns. In particular,  $\llbracket \lambda x. t \rrbracket^{-1}$  is not defined when  $x$  is not base typed, or  $\llbracket x(t_1, \dots, t_n) \rrbracket^{-1}$  is not defined when  $x$  is a bound variable.

Notice also that the permutation  $\pi$  is not completely determined by the side condition of the forth equation. For instance, given  $\langle a_1, a_2, a_3 \rangle$  as the list of atoms, all them of the same sort, to define  $\llbracket X(a_1) \rrbracket^{-1}_{\{a_1 \# X, a_2 \# X\}} = \pi^{-1}.X$  the condition requires  $\pi \cdot a_1 = a_3$ , but then, we can choose  $\pi \cdot a_2 = a_1$  and  $\pi \cdot a_3 = a_2$ , or vice versa  $\pi \cdot a_2 = a_2$  and  $\pi \cdot a_3 = a_1$ . Therefore,  $\llbracket t \rrbracket^{-1}_{\nabla}$  is nondeterministically defined.

For  $\lambda$ -substitutions the back-translation is defined as follows.

DEFINITION 7.2. Let  $\langle a_1, \dots, a_n \rangle$  be a fixed ordered list of atoms, and let  $\nabla$  be a freshness environment. The back-translation function is defined on  $\lambda$ -substitutions as follows.

$$\llbracket \sigma \rrbracket_{\nabla}^{-1} = \bigcup_{X \in \text{Dom}(\sigma)} \left[ X \mapsto \llbracket \sigma(X)(a_1, \dots, a_n) \rrbracket_{\nabla}^{-1} \right]$$

Notice that if  $\sigma(X)(a_1, \dots, a_n)$  is not a well-typed  $\lambda$ -term, or  $\llbracket \sigma(X)(a_1, \dots, a_n) \rrbracket_{\nabla}^{-1}$  is not defined for some  $X \in \text{Dom}(\sigma)$ , then  $\llbracket \sigma \rrbracket_{\nabla}^{-1}$  is not defined.

We introduce the following notion to describe which  $\lambda$ -terms and substitutions have reverse translation w.r.t. a freshness environment.

DEFINITION 7.3. Given a  $\lambda$ -term  $t$  (resp.  $\lambda$ -substitution  $\sigma$ ), and a freshness environment  $\nabla$ , we say that  $t$  (resp.  $\sigma$ ) is  $\nabla$ -compatible if  $\llbracket t \rrbracket_{\nabla}^{-1}$  (resp.  $\llbracket \sigma \rrbracket_{\nabla}^{-1}$ ) is defined.

LEMMA 7.4. For any  $\lambda$ -term  $t$ , and freshness environment  $\nabla$ , if  $t$  is  $\nabla$ -compatible, then  $\llbracket \llbracket t \rrbracket_{\nabla}^{-1} \rrbracket_{\nabla} = t$ .

For every  $\lambda$ -substitution  $\sigma$ , and freshness environment  $\nabla$ , if  $\sigma$  is  $\nabla$ -compatible, then  $\llbracket \llbracket \sigma \rrbracket_{\nabla}^{-1} \rrbracket_{\nabla} = \sigma$ .

PROOF. Let  $\langle a_1, \dots, a_n \rangle$  be a fixed ordered list of atoms. The existence of  $\llbracket t \rrbracket_{\nabla}^{-1}$  restricts the form of  $t$  to five cases. For the first four, the proof is trivial. In the case  $t = X(c_1, \dots, c_m)$ , we have

$$\begin{aligned} \llbracket \llbracket X(c_1, \dots, c_m) \rrbracket_{\nabla}^{-1} \rrbracket_{\nabla} &= \llbracket \pi^{-1} \cdot X \rrbracket_{\nabla} \\ &= X(\llbracket \pi^{-1} \cdot \pi \cdot c_1 \rrbracket_{\nabla}, \dots, \llbracket \pi^{-1} \cdot \pi \cdot c_m \rrbracket_{\nabla}) \\ &= X(c_1, \dots, c_m) \end{aligned}$$

where  $\pi$  is a permutation on  $\langle a_1, \dots, a_n \rangle$  satisfying  $\langle \pi \cdot c_1, \dots, \pi \cdot c_m \rangle$  is the sublist of  $\langle a_1, \dots, a_n \rangle$  such that  $\pi \cdot c_i \# X \notin \nabla$  and  $c_i$  and  $\pi \cdot c_i$  have the same sort.

For the second statement, by Definitions 7.2 and 5.8 we have

$$\begin{aligned} \llbracket \llbracket \sigma \rrbracket_{\nabla}^{-1} \rrbracket_{\nabla} &= \left[ \bigcup_{X \in \text{Dom}(\sigma)} [X \mapsto \llbracket \sigma(X)(a_1, \dots, a_n) \rrbracket_{\nabla}^{-1}] \right]_{\nabla} \\ &= \bigcup_{X \in \text{Dom}(\sigma)} \left[ X \mapsto \lambda a_1 \dots a_n. \llbracket \llbracket \sigma(X)(a_1, \dots, a_n) \rrbracket_{\nabla}^{-1} \rrbracket_{\nabla} \right] \\ &= \bigcup_{X \in \text{Dom}(\sigma)} [X \mapsto \lambda a_1 \dots a_n. \sigma(X)(a_1, \dots, a_n)] \\ &= \bigcup_{X \in \text{Dom}(\sigma)} [X \mapsto \sigma(X)] = \sigma \end{aligned}$$

Where we make use of the first statement to prove  $\llbracket \llbracket \sigma(X)(a_1, \dots, a_n) \rrbracket_{\nabla}^{-1} \rrbracket_{\nabla} = \sigma(X)(a_1, \dots, a_n)$ . Notice that, if  $\sigma$  is  $\nabla$ -compatible, then  $\sigma(X)(a_1, \dots, a_n)$  is also  $\nabla$ -compatible.  $\square$



Given a pattern unifier, in order to reconstruct the corresponding nominal unifier, we have several degrees of freedom. We start with higher-order pattern unifier  $\sigma$  with a restricted use of names of bound variables. Then, we will construct a freshness environment  $\nabla$  such that  $\sigma$  is  $\nabla$ -compatible. This construction is described in the proof of Lemma 7.6, and it is nondeterministic. The corresponding nominal solution is then  $\langle \nabla, \llbracket \sigma \rrbracket_{\nabla}^{-1} \rangle$ . Moreover,  $\llbracket \sigma \rrbracket_{\nabla}^{-1}$  is not uniquely defined. The following example illustrates these degrees of freedom in this back-translation.

EXAMPLE 7.5. The nominal unification problem

$$P = \{a.a.X \stackrel{?}{\approx} c.a.X, a.b.X \stackrel{?}{\approx} b.a.(a b).X\}$$

where all atoms and variables are of the same sort, is translated as

$$\llbracket P \rrbracket = \{ \lambda a.\lambda b.\lambda c.\lambda a.\lambda a.X(a, b, c) \stackrel{?}{=} \lambda a.\lambda b.\lambda c.\lambda c.\lambda a.X(a, b, c), \\ \lambda a.\lambda b.\lambda c.\lambda a.\lambda b.X(a, b, c) \stackrel{?}{=} \lambda a.\lambda b.\lambda c.\lambda b.\lambda a.X(b, a, c) \}$$

Most general higher-order pattern unifiers are

$$\sigma_1 = [X \mapsto \lambda a.\lambda b.\lambda c.Z(a, b)]$$

and

$$\sigma_2 = [X \mapsto \lambda a.\lambda b.\lambda c.Z(b, a)]$$

which are equivalent.

Let  $\langle a, b, c \rangle$  be the fixed list of atoms. Following the construction described in the forthcoming proof of Lemma 7.6, for every variable  $Z$  occurring in  $\sigma$ , we construct a sublist of atoms  $L_Z = \langle b_1, \dots, b_m \rangle$  satisfying  $b_j : \llbracket \tau_j \rrbracket^{-1}$ , for every  $j = 1, \dots, m$ . In our case, we can choose among three possibilities  $L_Z^1 = \langle a, b \rangle$ ,  $L_Z^2 = \langle a, c \rangle$  or  $L_Z^3 = \langle b, c \rangle$ . We construct  $\nabla = \bigcup_{\substack{Z \text{ occurs in } \sigma \\ a \in \langle a_1, \dots, a_n \rangle \setminus L_Z}} \{a \# Z\}$ .

From the two pattern unifiers  $\sigma_i$ 's, and the three lists  $L_Z^j$ 's we can construct six possible nominal unifiers:

	$\sigma_1$	$\sigma_2$
$L_Z^1$	$\langle \{c \# Z\}, [X \mapsto \left( \begin{smallmatrix} a & b & c \\ a & b & c \end{smallmatrix} \right)^{-1} \cdot Z] \rangle$	$\langle \{c \# Z\}, [X \mapsto \left( \begin{smallmatrix} a & b & c \\ b & a & c \end{smallmatrix} \right)^{-1} \cdot Z] \rangle$
$L_Z^2$	$\langle \{b \# Z\}, [X \mapsto \left( \begin{smallmatrix} a & b & c \\ a & c & b \end{smallmatrix} \right)^{-1} \cdot Z] \rangle$	$\langle \{b \# Z\}, [X \mapsto \left( \begin{smallmatrix} a & b & c \\ c & a & b \end{smallmatrix} \right)^{-1} \cdot Z] \rangle$
$L_Z^3$	$\langle \{a \# Z\}, [X \mapsto \left( \begin{smallmatrix} a & b & c \\ b & c & a \end{smallmatrix} \right)^{-1} \cdot Z] \rangle$	$\langle \{a \# Z\}, [X \mapsto \left( \begin{smallmatrix} a & b & c \\ c & b & a \end{smallmatrix} \right)^{-1} \cdot Z] \rangle$

The permutations can be written as swappings obtaining:

	$\sigma_1$	$\sigma_2$
$L_Z^1$	$\langle \{c \# Z\}, [X \mapsto Z] \rangle$	$\langle \{c \# Z\}, [X \mapsto (a b) \cdot Z] \rangle$
$L_Z^2$	$\langle \{b \# Z\}, [X \mapsto (b c) \cdot Z] \rangle$	$\langle \{b \# Z\}, [X \mapsto (a b)(b c) \cdot Z] \rangle$
$L_Z^3$	$\langle \{a \# Z\}, [X \mapsto (a c)(b c) \cdot Z] \rangle$	$\langle \{a \# Z\}, [X \mapsto (a c) \cdot Z] \rangle$

All these nominal unifiers are most general and equivalent. Notice that these are *all* the most general nominal unifiers.

LEMMA 7.6. *For every equational nominal unification problem  $P$ , if the pattern unification problem  $\llbracket P \rrbracket$  is solvable, then there exists a freshness environment  $\nabla$ , and a most general pattern unifier  $\sigma$ , such that  $\sigma$  is  $\nabla$ -compatible.*

PROOF. The most general unifier  $\sigma$  is chosen, accordingly to Lemma 6.11, as a unifier not using other bound variable names than the ones used in  $\llbracket P \rrbracket$ . Moreover, since all bound variables of  $\llbracket P \rrbracket$  with the same name  $a_i$  have the same type  $\tau_i$ , the same happens in  $\sigma$ , and all free variables  $Z$  occurring in  $\sigma$  have a type of the form  $Z : \tau_{i_1} \rightarrow \dots \rightarrow \tau_{i_m} \rightarrow \delta$ , for some indexes satisfying  $1 \leq i_1 < \dots < i_m \leq n$ . Notice that there could be more than one set of indexes satisfying this condition.

The freshness environment  $\nabla$  is constructed as follows. For any variable  $Z : \tau_{i_1} \rightarrow \dots \tau_{i_m} \rightarrow \delta$  occurring<sup>6</sup> in  $\sigma$ , let  $L_Z = \langle \mathbf{a}_{i_1}, \dots, \mathbf{a}_{i_m} \rangle$  be a sublist of the atoms  $\langle \mathbf{a}_1, \dots, \mathbf{a}_n \rangle$ . Then,

$$\nabla = \bigcup_{\substack{Z \text{ occurs in } \sigma \\ \mathbf{a} \in \langle \mathbf{a}_1, \dots, \mathbf{a}_n \rangle \setminus L_Z}} \{\mathbf{a} \# Z\}$$

We prove that  $\sigma(X)(a_1, \dots, a_n)$  is  $\nabla$ -compatible, for any  $X \in \text{Dom}(\sigma)$ .

Since  $\sigma$  is most general  $\text{Dom}(\sigma)$  only contains variables  $X$  of  $\llbracket P \rrbracket$ . All these variables have type  $\llbracket \tau_1 \rrbracket \rightarrow \dots \rightarrow \llbracket \tau_n \rrbracket \rightarrow \llbracket \tau_0 \rrbracket$ , where  $\langle \tau_1, \dots, \tau_n \rangle$  is the list of sorts of  $\langle \mathbf{a}_1, \dots, \mathbf{a}_n \rangle$ , and  $\tau_0$  is the sort of  $\mathbf{X}$ . Therefore,  $\sigma(X)(a_1, \dots, a_n)$  is a well-typed  $\lambda$ -term. Now we prove that this term is *back-translatable* by structural induction.

By Lemma 6.11,  $\sigma(X)$  does not use bound variables with other names and types than the ones already used in the original problem. This ensures that we can always translate back bound variables  $a$  as the atom with the same name  $\mathbf{a}$ . Terms formed by a constant or free variable are particular cases of applications with  $m = 0$ , studied bellow.

All  $\lambda$ -abstractions will be of the form  $\lambda a_i. t$ , where  $a_i = \llbracket \mathbf{a}_i \rrbracket$ . This ensure that its translation back is possible, if the body of the  $\lambda$ -abstractions is back-translatable.

All applications are of the form  $f(t_1, \dots, t_m)$  where  $f$  is a constant of the original nominal problem (since  $\sigma$  is most general), or of the form  $X(a_{i_1}, \dots, a_{i_m})$  where  $X$  is a free variable and  $a_{i_1}, \dots, a_{i_m}$  are distinct bound variables. Notice that we can no have terms of the form  $a_i(t_1, \dots, t_n)$  where  $a_i$  is a bound variable, because all these bound variables have basic types. In the first case, the application is back-translatable if arguments are. In the second case, let  $X : \tau_{j_1} \rightarrow \dots \rightarrow \tau_{j_m} \rightarrow \delta$ , for some indexes satisfying  $1 \leq j_1 < \dots < j_m \leq n$ . using the  $\nabla$  constructed before, we can translate back  $X(a_{i_1}, \dots, a_{i_m})$  as  $\pi^{-1} \cdot \mathbf{X}$ , for some  $\pi$  satisfying  $\pi(\mathbf{a}_{i_k}) = \mathbf{a}_{j_k}$ , for  $j = 1, \dots, m$ . Notice that  $\mathbf{a}_{j_k}$  and  $\mathbf{a}_{i_k}$  have the same sort  $\tau_{j_k}$ . Hence, this second kind of applications is also back-translatable.  $\square$

THEOREM 7.7. *For every equational nominal unification problem  $P$ , if the pattern unification problem  $\llbracket P \rrbracket$  is solvable, then  $P$  is also solvable.*

PROOF. By Lemma 7.6, if  $\llbracket P \rrbracket$  is solvable then there exist a most general unifier  $\sigma$  of  $\llbracket P \rrbracket$ , and a freshness environment  $\nabla$  such that  $\langle \nabla, \llbracket \sigma \rrbracket^{-1}_{\nabla} \rangle$  is defined. W.l.o.g. assume that  $\text{Dom}(\sigma) = \text{Vars}(\llbracket P \rrbracket)$  and hence, according to Definition 7.2,

<sup>6</sup>We say that  $X$  occurs in  $\sigma$ , if  $X$  occurs free in  $\sigma(Y)$ , for some  $Y \in \text{Dom}(\sigma)$ .

$\text{Dom}(\llbracket \sigma \rrbracket_{\nabla}^{-1}) = \text{Vars}(P)$ . By Lemma 7.4, we have  $\llbracket \llbracket \sigma \rrbracket_{\nabla}^{-1} \rrbracket_{\nabla} = \sigma$ , which solves  $\llbracket P \rrbracket$ . Hence, by Theorem 5.13,  $\langle \nabla, \llbracket \sigma \rrbracket_{\nabla}^{-1} \rangle$  solves  $P$ .  $\square$

From Theorems 5.15 and 7.7, and linear-time decidability for Higher-Order Patterns Unification [Qian 1996], we conclude the following results.

**COROLLARY 7.8.** *Nominal Unification is quadratic reducible to Higher-Order Pattern Unification.*

*Nominal Unification can be decided in quadratic deterministic time.*

## 8. CORRESPONDENCE BETWEEN UNIFIERS

In this section we establish a correspondence between the solutions of a nominal unification problem and their translations. We prove that the translation function is monotone, in the sense that it translates more general nominal solutions into more general pattern solutions. The reverse translation also satisfies this property. Therefore, both translate most general solutions into most general solutions. We start by generalizing the translation of a nominal substitution w.r.t. a freshness environment, to respect the translation of a nominal substitution w.r.t. *two* freshness environments, and similarly for the reverse translation.

**DEFINITION 8.1.** *Let  $\langle a_1, \dots, a_n \rangle$  be a fixed list of atoms.*

*Given a nominal substitution  $\sigma$ , and two freshness environments  $\nabla$  and  $\nabla'$ , satisfying  $\nabla \vdash \sigma(\nabla')$ , we define*

$$\llbracket \sigma \rrbracket_{\nabla}^{\nabla'} = \bigcup_{X \in \text{Dom}(\sigma)} [X \mapsto \lambda b_1, \dots, b_m. \llbracket \sigma(X) \rrbracket_{\nabla}]$$

where  $\langle b_1, \dots, b_m \rangle = \langle a \in \langle a_1, \dots, a_n \rangle \mid a \# X \notin \nabla' \rangle$ .

*Given a pattern substitution  $\sigma$ , and two freshness environments  $\nabla$  and  $\nabla'$ , we define*

$$\llbracket \sigma \rrbracket_{\nabla}^{-1 \nabla'} = \bigcup_{X \in \text{Dom}(\sigma)} [X \mapsto \llbracket \sigma(X)(b_1, \dots, b_m) \rrbracket_{\nabla}^{-1}]$$

where  $\langle b_1, \dots, b_m \rangle = \langle a \in \langle a_1, \dots, a_n \rangle \mid a \# X \notin \nabla' \rangle$ .

*We say that  $\sigma$  is  $\nabla' \rightarrow \nabla$ -compatible if  $\llbracket \sigma \rrbracket_{\nabla}^{-1 \nabla'}$  exists.*

Notice that this definition generalizes Definition 5.8 because  $\llbracket \sigma \rrbracket_{\nabla} = \llbracket \sigma \rrbracket_{\nabla}^{\emptyset}$ , and Definition 7.2 because,  $\llbracket \sigma \rrbracket_{\nabla}^{-1} = \llbracket \sigma \rrbracket_{\nabla}^{-1 \emptyset}$ .

The following lemmas are generalizations of Lemmas 5.11 and 7.4, respectively. Their proofs are also straightforward generalizations.

**LEMMA 8.2.** *For any nominal substitution  $\sigma$ , freshness environments  $\nabla_1$  and  $\nabla_2$ , and nominal term  $t$ , satisfying  $\nabla_2 \vdash \sigma(\nabla_1)$  and  $\text{Vars}(t) \subseteq \text{Dom}(\sigma)$ , we have*

$$\llbracket \sigma \rrbracket_{\nabla_2}^{\nabla_1}(\llbracket t \rrbracket_{\nabla_1}) = \llbracket \sigma(t) \rrbracket_{\nabla_2}$$

**LEMMA 8.3.** *For any  $\lambda$ -substitution  $\sigma$  and freshness environment  $\nabla_1$  and  $\nabla_2$ , if  $\sigma$  is  $\nabla_1 \rightarrow \nabla_2$ -compatible, then*

$$\llbracket \llbracket \sigma \rrbracket_{\nabla_2}^{-1 \nabla_1} \rrbracket_{\nabla_2}^{\nabla_1} = \sigma$$

If a  $\lambda$ -substitution  $\sigma_1$  is more general than another  $\sigma_2$ , then there exists a substitution  $\sigma_3$  that satisfies  $\sigma_2 = \sigma_3 \circ \sigma_1$ . The following lemma states that this substitution can be used to construct a nominal substitution  $\llbracket \sigma_3 \rrbracket^{-1}$  that we will use, in Lemma 8.5, to prove that  $\llbracket \sigma_1 \rrbracket^{-1}$  is more general than  $\llbracket \sigma_2 \rrbracket^{-1}$ .

LEMMA 8.4. *For any pair of  $\lambda$ -substitutions  $\sigma_1$  and  $\sigma_2$  and freshness environments  $\nabla_1$  and  $\nabla_2$ , if  $\sigma_1$  is  $\nabla_1$ -compatible,  $\sigma_2$  is  $\nabla_2$ -compatible, and  $\sigma_1$  is more general than  $\sigma_2$ , then there exists a  $\lambda$ -substitution  $\sigma_3$  such that*

- (1)  $\sigma_2 = \sigma_3 \circ \sigma_1|_{\text{Dom}(\sigma_1) \cup \text{Dom}(\sigma_2)}$
- (2)  $\sigma_3$  is  $\nabla_1 \rightarrow \nabla_2$ -compatible, and
- (3)  $\nabla_2 \vdash \llbracket \sigma_3 \rrbracket^{-1}_{\nabla_2} \nabla_1$ .

PROOF. The first conclusion is a consequence of  $\sigma_1$  is more general than  $\sigma_2$ . However, w.l.o.g. we take a  $\sigma_3$  that only instantiates variables occurring in  $\sigma_1$  or belonging to  $\text{Dom}(\sigma_2)$ .

For all  $X \in \text{Dom}(\sigma_3)$ , let  $\langle \mathbf{b}_1, \dots, \mathbf{b}_m \rangle = \langle \mathbf{a}_i \mid \mathbf{a}_i \# X \notin \nabla_1 \rangle$ , where  $\langle \mathbf{a}_1, \dots, \mathbf{a}_n \rangle$  is the fixed list of atom names. Now,  $X$  occurs in  $\sigma_1$  or  $X \in \text{Dom}(\sigma_2)$ . In the first case, since  $\sigma_1$  is  $\nabla_1$ -compatible and we are dealing with higher-order pattern substitutions,  $X$  occurs in  $\sigma_1$  in (at least one) subterm of the form  $X(b'_1, \dots, b'_m)$ , where  $b'_i$  are distinct bound variables with names in  $\langle \mathbf{a}_1, \dots, \mathbf{a}_n \rangle$ , and  $b_i$  and  $b'_i$  have the same type. Moreover,  $\sigma_3(X)(b'_1, \dots, b'_m)$ , conveniently  $\beta$ -reduced, is a subterm of some  $\sigma_2(Y)$ , for some  $Y \in \text{Dom}(\sigma_2)$ . In the second case, if  $X \in \text{Dom}(\sigma_2)$ , we also have this property. Therefore, since  $\sigma_2$  is  $\nabla_2$ -compatible, we have that  $\sigma_3(X)(b'_1, \dots, b'_m)$ , and hence  $\sigma_3(X)(b_1, \dots, b_m)$  is  $\nabla_2$ -compatible. Therefore,  $\llbracket \sigma_3 \rrbracket^{-1}_{\nabla_2} = \bigcup_{X \in \text{Dom}(\sigma_3)} [X \mapsto \llbracket \sigma_3(X)(b_1, \dots, b_m) \rrbracket^{-1}]$  exists, and  $\sigma_3$  is  $\nabla_1 \rightarrow \nabla_2$ -compatible.

Let be  $\mathbf{b} \# X \in \nabla_1$ . The free variable names of  $\sigma_3(X)$  and  $\langle \mathbf{a}_1, \dots, \mathbf{a}_n \rangle$  are disjoint. Therefore,  $b \notin \text{FV}(\sigma_3(X)(b_1, \dots, b_m))$ , where  $\langle \mathbf{b}_1, \dots, \mathbf{b}_m \rangle = \langle \mathbf{a}_i \mid \mathbf{a}_i \# X \notin \nabla_1 \rangle$ . By Lemma 7.4, since  $\sigma_3(X)(b_1, \dots, b_m)$  is  $\nabla_2$ -compatible, we have  $b \notin \text{FV} \left( \llbracket \llbracket \sigma_3(X)(b_1, \dots, b_m) \rrbracket^{-1}_{\nabla_2} \rrbracket_{\nabla_2} \right)$ . By Lemma 5.10,  $\nabla_2 \vdash \mathbf{b} \# \llbracket \sigma_3(X)(b_1, \dots, b_m) \rrbracket^{-1}_{\nabla_2}$ . By Definition 8.1,  $\nabla_2 \vdash \mathbf{b} \# \llbracket \sigma_3 \rrbracket^{-1}_{\nabla_2} (X)$ . Therefore, we have  $\nabla_2 \vdash \llbracket \sigma_3 \rrbracket^{-1}_{\nabla_2} \nabla_1$ .  $\square$

The following lemma ensures that the translation and reverse translation of substitutions is monotone w.r.t. the more generality relation.

LEMMA 8.5. *For every nominal unification problem  $P$  and pair of unifiers  $\langle \nabla_1, \sigma_1 \rangle$  and  $\langle \nabla_2, \sigma_2 \rangle$ , satisfying  $\text{Vars}(P) \subseteq \text{Dom}(\sigma_1) \subseteq \text{Dom}(\sigma_2)$ , we have  $\langle \nabla_1, \sigma_1 \rangle$  is more general than  $\langle \nabla_2, \sigma_2 \rangle$ , if, and only if,  $\llbracket \sigma_1 \rrbracket_{\nabla_1}$  is more general than  $\llbracket \sigma_2 \rrbracket_{\nabla_2}$ .*

PROOF.  $\Rightarrow$ ) By Theorem 5.13, both  $\llbracket \sigma_1 \rrbracket_{\nabla_1}$  and  $\llbracket \sigma_2 \rrbracket_{\nabla_2}$  are solutions of  $[P]$ . If  $\langle \nabla_1, \sigma_1 \rangle$  is more general than  $\langle \nabla_2, \sigma_2 \rangle$ , then there exists a nominal substitution  $\sigma'$  such that  $\nabla_2 \vdash \sigma'(\nabla_1)$  and  $\nabla_2 \vdash \sigma' \circ \sigma_1|_{\text{Dom}(\sigma_1) \cup \text{Dom}(\sigma_2)} \approx \sigma_2$ . For all  $X \in \text{Dom}(\sigma_2)$ , we have  $\nabla_2 \vdash \sigma'(\sigma_1(X)) \approx \sigma_2(X)$ . By Lemma 5.10,  $\llbracket \sigma'(\sigma_1(X)) \rrbracket_{\nabla_2} =_\alpha \llbracket \sigma_2(X) \rrbracket_{\nabla_2}$ . By Lemma 8.2,  $\llbracket \sigma' \rrbracket_{\nabla_2}^{\nabla_1} (\llbracket \sigma_1(X) \rrbracket_{\nabla_1}) =_\alpha \llbracket \sigma_2(X) \rrbracket_{\nabla_2}$ . By Lemma 5.11,

$\llbracket \sigma' \rrbracket_{\nabla_2}^{\nabla_1}(\llbracket \sigma_1 \rrbracket_{\nabla_1}(\llbracket X \rrbracket_{\emptyset})) =_{\alpha} \llbracket \sigma_2 \rrbracket_{\nabla_2}(\llbracket X \rrbracket_{\emptyset})$ . Since  $\llbracket X \rrbracket_{\emptyset} = X(a_1, \dots, a_n)$  and  $a_i$  will be distinct free variables, we have

$$\llbracket \sigma_2 \rrbracket_{\nabla_2}(X) = \llbracket \sigma' \rrbracket_{\nabla_2}^{\nabla_1} \circ \llbracket \sigma_1 \rrbracket_{\nabla_1}(X), \quad \text{for all } X \in \text{Dom}(\llbracket \sigma_2 \rrbracket_{\nabla_2})$$

Therefore,  $\llbracket \sigma_1 \rrbracket_{\nabla_1}$  is more general than  $\llbracket \sigma_2 \rrbracket_{\nabla_2}$ .

$\Leftarrow$ ) There exists a  $\lambda$ -substitution  $\sigma'$  such that  $\llbracket \sigma_2 \rrbracket_{\nabla_2} = \sigma' \circ \llbracket \sigma_1 \rrbracket_{\nabla_1}|_{\text{Dom}(\sigma_1) \cup \text{Dom}(\sigma_2)}$ . By Lemma 8.4,  $\sigma'$  is  $\nabla_1 \rightarrow \nabla_2$ -compatible. Hence, it exists the nominal substitution  $\sigma'' = \llbracket \sigma' \rrbracket_{\nabla_2}^{-1 \nabla_1}$ . For any  $X \in \text{Dom}(\sigma_2)$ , by Lemmas 8.2 and 8.3, we have  $\llbracket \sigma''(\sigma_1(X)) \rrbracket_{\nabla_2} = \llbracket \sigma'' \rrbracket_{\nabla_2}^{\nabla_1}(\llbracket \sigma_1 \rrbracket_{\nabla_1}^{\emptyset}(\llbracket X \rrbracket_{\emptyset})) = \sigma'(\llbracket \sigma_1 \rrbracket_{\nabla_1}^{\emptyset}(\llbracket X \rrbracket_{\emptyset})) = \llbracket \sigma_2 \rrbracket_{\nabla_2}^{\emptyset}(\llbracket X \rrbracket_{\emptyset}) = \llbracket \sigma_2(X) \rrbracket_{\nabla_2}$ . By Lemma 5.10, we have  $\nabla_2 \vdash \sigma''(\sigma_1(X)) \approx \sigma_2(X)$ . Therefore,  $\nabla_2 \vdash \sigma'' \circ \sigma_1|_{\text{Dom}(\sigma_1) \cup \text{Dom}(\sigma_2)} \approx \sigma_2$ . By Lemma 8.4, we also have  $\nabla_2 \vdash \sigma''(\nabla_1)$ . From both facts, we conclude that  $\sigma_1$  is more general than  $\sigma_2$ .  $\square$

**COROLLARY 8.6.** *Most general nominal unifiers are unique.*

**PROOF.** It is a direct consequence of uniqueness of most general higher-order pattern unifiers and Lemma 8.5.  $\square$

Finally we can conclude that the translations preserve most generality.

**THEOREM 8.7.** *For any nominal problem  $P$  and nominal solution  $\langle \nabla, \sigma \rangle$ , satisfying  $\text{Vars}(P) \subseteq \text{Dom}(\sigma)$ ,  $\langle \nabla, \sigma \rangle$  is a most general unifier if, and only if,  $\llbracket \sigma \rrbracket_{\nabla}$  is a most general unifier of  $\llbracket P \rrbracket$ .*

**PROOF.**  $\Rightarrow$ ) Suppose that  $\langle \nabla, \sigma \rangle$  is a most general nominal unifier of  $P$ , but  $\llbracket \sigma \rrbracket_{\nabla}$  is not a most general pattern unifier of  $\llbracket P \rrbracket$ . By Theorem 5.13,  $\llbracket \sigma \rrbracket_{\nabla}$  is a solution of  $\llbracket P \rrbracket$ . Since most general higher-order pattern unifiers are unique, and by Lemma 7.6, there exists a most general pattern unifier  $\sigma'$  of  $\llbracket P \rrbracket$  *strictly* more general than  $\llbracket \sigma \rrbracket_{\nabla}$  and such that  $\llbracket \sigma' \rrbracket^{-1}$  exists. By Lemma 7.4,  $\llbracket \llbracket \sigma' \rrbracket^{-1} \rrbracket = \sigma'$ . Since we assume that  $\langle \nabla, \sigma \rangle$  is most general and nominal most general unifiers are also unique, we have that  $\langle \nabla, \sigma \rangle$  is more general than  $\llbracket \sigma' \rrbracket^{-1}$ . Hence, by Lemma 8.5,  $\llbracket \sigma \rrbracket_{\nabla}$  is more general than  $\llbracket \llbracket \sigma' \rrbracket^{-1} \rrbracket = \sigma'$ , which contradicts that  $\sigma'$  is strictly more general than  $\llbracket \sigma \rrbracket_{\nabla}$ .

$\Leftarrow$ ) Suppose that  $\llbracket \sigma \rrbracket_{\nabla}$  is most general, and  $\langle \nabla, \sigma \rangle$  is not. Then, there exists a most general unifier  $\langle \nabla', \sigma' \rangle$  such that  $\langle \nabla, \sigma \rangle$  is not more general than  $\langle \nabla', \sigma' \rangle$ . On the other hand, since  $\llbracket \sigma \rrbracket_{\nabla}$  is most general, it is more general than  $\llbracket \sigma' \rrbracket_{\nabla'}$ . Hence, by Lemma 8.5,  $\langle \nabla, \sigma \rangle$  is more general than  $\langle \nabla', \sigma' \rangle$ . This contradicts the initial assumption. Therefore, if  $\llbracket \sigma \rrbracket_{\nabla}$  is most general, then  $\langle \nabla, \sigma \rangle$  must be most general.  $\square$

## 9. CONCLUSIONS

The paper describes a precise quadratic reduction from Nominal Unification to Higher-Order Pattern Unification. This helps to better understand the semantics of the nominal binding and permutations in comparison with  $\lambda$ -binding and  $\alpha$ -conversion. Moreover, using the result of linear time decidability for Higher-Order Patterns Unification [Qian 1996], we prove that Nominal Unification can be decided in quadratic time.

## REFERENCES

- CALVÈS, C. 2010. Complexity and implementation of nominal algorithms. Ph.D. thesis, King's College London.
- CALVÈS, C. AND FERNÁNDEZ, M. 2007. Implementing nominal unification. *ENTCS* 176, 1, 25–37.
- CALVÈS, C. AND FERNÁNDEZ, M. 2008. A polynomial nominal unification algorithm. *Theoretical Computer Science* 403, 2-3, 285–306.
- CHENEY, J. 2005a. Equivariant unification. In *Proc. of the 16th Int. Conf. on Rewriting Techniques and Applications, RTA'05*. Lecture Notes in Computer Science, vol. 3467. Springer, 74–89.
- CHENEY, J. 2005b. Relating higher-order pattern unification and nominal unification. In *Proc. of the 19th Int. Work. on Unification, UNIF'05*. 104–119.
- CHENEY, J. AND URBAN, C. 2004.  $\alpha$ -prolog: A logic programming language with names, binding and  $\alpha$ -equivalence. In *Proc. of the 20th Int. Conf. on Logic Programming, ICLP'04*. LNCS, vol. 3132. 269–283.
- CLOUSTON, R. A. AND PITTS, A. M. 2007. Nominal equational logic. *ENTCS* 1496, 223–257.
- DOWEK, G. 2001. Higher-order unification and matching. In *Handbook of automated reasoning*. 1009–1062.
- DOWEK, G., GABBAY, M., AND MULLIGAN, D. 2010. Permissive nominal terms and their unification. *Logic Journal of the IGPL*.
- DOWEK, G., GABBAY, M. J., AND MULLIGAN, D. 2009. Permissive nominal terms and their unification. In *Proc. of the 24th Italian Conf. on Computational Logic, CILC'09*.
- FERNÁNDEZ, M. AND GABBAY, M. 2005. Nominal rewriting with name generation: abstraction vs. locality. In *Proc. of the 7th Int. Conf. on Principles and Practice of Declarative Programming, PPDP'05*. 47–58.
- FERNÁNDEZ, M. AND GABBAY, M. 2007. Nominal rewriting. *Information and Computation* 205, 6, 917–965.
- GABBAY, M. AND MATHIJSEN, A. 2006. Nominal algebra. In *Proc. of the 18th Nordic Workshop on Programming Theory, NWPT'06*.
- GABBAY, M. AND MATHIJSEN, A. 2007. A formal calculus for informal equality with binding. In *Logic, Language, Information and Computation*. LNCS, vol. 4576. Springer, 162–176.
- GABBAY, M. AND MATHIJSEN, A. 2009. Nominal (universal) algebra: equational logic with names and binding. *Journal of Logic and Computation* 19, 6, 1455–1508.
- GABBAY, M. AND PITTS, A. 2001. A new approach to abstract syntax with variable binding. *Formal Aspects of Computing* 13, 3–5, 341–363.
- GABBAY, M. AND PITTS, A. M. 1999. A new approach to abstract syntax involving binders. In *Proc. of the 14th Symp. on Logic in Computer Science, LICS'99*. 214–224.
- GOLDFARB, W. D. 1981. The undecidability of the second-order unification problem. *Theoretical Computer Science* 13, 225–230.
- LEVY, J. 1998. Decidable and undecidable second-order unification problems. In *Proc. of the 9th Int. Conf. on Rewriting Techniques and Applications, RTA'98*. LNCS, vol. 1379. 47–60.
- LEVY, J. AND VEANES, M. 2000. On the undecidability of second-order unification. *Information and Computation* 159, 125–150.
- LEVY, J. AND VILLARET, M. 2008. Nominal unification from a higher-order perspective. In *Proc. of the 19th Int. Conf. on Rewriting Techniques and Applications, RTA'08*. LNCS, vol. 5117. Springer, 246–260.
- LEVY, J. AND VILLARET, M. 2010. An efficient nominal unification algorithm. In *Proc. of the 21th Int. Conf. on Rewriting Techniques and Applications, RTA'10*. LNCS. Springer.
- LUCCHESI, C. L. 1972. The undecidability of the unification problem for third-order languages. Tech. Rep. CSRR 2059, Dept. of Applied Analysis and Computer Science, Univ. of Waterloo.
- MILLER, D. 1991. A logic programming language with lambda-abstraction, function variables, and simple unification. *J. of Logic and Computation* 1, 4, 497–536.
- NIPKOW, T. 1993. Functional unification of higher-order patterns. In *Proc. of the 8th Symp. on Logic in Computer Science, LICS'93*. 64–74.
- ACM Transactions on Computational Logic, Vol. V, No. N, Month 20YY.

- PATERSON, M. AND WEGMAN, M. N. 1978. Linear unification. *J. Comput. Syst. Sci.* 16, 2, 158–167.
- PITTS, A. M. 2001. Nominal logic: A first order theory of names and binding. In *Proc. of the 4th Int. Symp. on Theoretical Aspects of Computer Software, TACS'01*. LNCS, vol. 2215. 219–242.
- PITTS, A. M. 2003. Nominal logic, a first order theory of names and binding. *Information and Computation* 186, 165–193.
- QIAN, Z. 1996. Unification of higher-order patterns in linear time and space. *J. of Logic and Computation* 6, 3, 315–341.
- URBAN, C. AND CHENEY, J. 2005. Avoiding equivariance in alpha-prolog. In *Proc. of the Int. Conf. on Typed Lambda Calculus and Applications, TLCA'05*. LNCS, vol. 3461. 401–416.
- URBAN, C., PITTS, A. M., AND GABBAY, M. J. 2003. Nominal unification. In *Proc. of the 17th Int. Work. on Computer Science Logic, CSL'03*. LNCS, vol. 2803. 513–527.
- URBAN, C., PITTS, A. M., AND GABBAY, M. J. 2004. Nominal unification. *Theoretical Computer Science* 323, 473–497.